BY ORDER OF THE COMMANDER
AIR MOBILITY COMMAND

AIR MOBILITY COMMAND PAMPHLET 14-104

9 OCTOBER 2003

Intelligence

AIR MOBILITY COMMAND INTELLIGENCE HANDBOOK

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: HQ AMC/INXU (Maj Alice E. Prichard)

Certified by: HQ AMC/INX
(Lt Col Linda M. Christiansen)

Supersedes AMCPAM14-104, 15 August 1997

Pages: 173
Distribution: F

This pamphlet is intended to provide AMC intelligence professionals with the basic tools needed to provide quality intelligence support. It is designed to compliment, not replace, Air Force and AMC instructions and supplements. Our goal is to assist the reader to understand and fully satisfy mission and regulatory requirements. This edition supersedes all previously issued "Cookbooks." E-mail recommendations to change, add, or delete information in this pamphlet to: **mailto:AMC.INXU@scott.af.mil** or mail hard copy to the following address: HQ AMC/INXU, 402 SCOTT DRIVE, UNIT 1L8, SCOTT AFB IL 62225-5309

Chapter 1

LEADERSHIP AND MANAGEMENT

1.1. General. This chapter provides information to help develop the framework required for the smooth operation of your intelligence flight. The three principal topics covered include: Internal Management, Personnel Management, and the Individual Mobilization Augmentee (IMA) Program Management.

1.2. Internal Management. This function is vital to intelligence mission success. Comprehensive Operational Instructions (OIs), checklists, continuity books, and other written guidance can facilitate standardized procedures and help to ensure adequate performance levels in spite of personnel turnovers, shortages, and increased operations tempo. Have resident experts on particular processes put their knowledge into a continuity book and checklist.

1.2.1. Continuity Files. Good continuity files are critical for long-term success. These files can help unit personnel avoid the mistakes of their predecessors and build upon their good ideas. A basic continuity file should have two sections. The first section includes higher headquarters guidance while the second section includes local guidance and other various items of interest. A more robust continuity file would include a continuity folder, or binder, for each program. A comprehensive program continuity binder should contain 5 sections:

1.2.1.1. Introduction. The introduction describes the program and identifies overall goals. It defines the program and discusses its importance. The introduction should also list governing directives/guidance, identify supporting agencies, and document the last review date.

1.2.1.2. Table of Contents.

1.2.1.3. Tasks. This section should provide a comprehensive list and description of all recurring and periodic tasks associated with the program. Tasks may be broken out as daily, weekly, monthly, annual, and as required. The specific level of detail and breakout will depend on the program described.

1.2.1.4. Self-Assessment/Program Review. Completed self-assessment/program review checklists from at least the most recent iteration should be kept in the continuity binder. This provides an "at a glance" picture of where the program is at any time, as well as areas locally identified for improvement.

1.2.1.5. Guidance and Direction. Copies of pertinent Higher Headquarters (HHQ) guidance and direction (Department of Defense (DoD) Dir, AFI, AMCI, etc.) should be kept with the program continuity binder.

1.2.2. Higher Headquarters Guidance and Direction. Apart from specific program continuity files, each unit should also maintain a centrally located, easily accessible, master set of instructions. Specific requirements will vary by unit and mission, but we recommend the following instructions/directions as the essential minimum:

- AFPD 14-1, *Intelligence Applications and Requirements Planning*
- AFPD 14-3, *Control, Protection, and Dissemination of Intelligence Information*
- AFI 14-103, *Threat Recognition Training Program*

- AFI 14-104, *Oversight of Intelligence Activities*
- AFI 14-105, *Unit Intelligence Mission and Responsibilities and AMC Sup 1*
- AFI 14-106, *Intelligence Education, Research, and Training Programs*
- AFI 14-201, *Intelligence Production and Applications*
- AFI 33-360 V I, *Publications Management Program*
- AFI 90-201, *Inspector General Activities*
- AFPAM 14-118, *Aerospace Intelligence Preparation of the Battlespace*
- AMCI 14-102, *Debriefing and Reporting*
- AMCI 14-103, *Requesting Intelligence Information and Imagery*
- AMCPAM 14-104, *AMC Intelligence Handbook*
- AMCI 14-106, *Threat Working Group*
- AMCI 14-107, *Command Intelligence Training Program*
- AMCI 90-201, *The Inspection System*
- AMCPAM 90-202, *The Inspection Guide*
- AMC Task List, version 1.0, 15 Apr 99 (**https://www.amc.af.mil/do/do.cfm**), (JTS/METLs)
- Training manuals and operating procedures for computer and communications devices

1.2.3. Unit Information, Guidance, and Direction. Each unit must develop guidance and instructions, tailored to unit organization and mission, detailing responsibilities, processes, and procedures required for accomplishing the mission. As with HHQ direction, a master copy should be centrally maintained and readily accessible to all assigned. As a minimum, we recommend the following:

- Flight organization (showing functional responsibilities)
- Accurate job descriptions for each authorized position
- Copy of organization and functions briefing
- Personnel management procedures
- Manpower authorization change procedures
- Intelligence mobility procedures
- Current unit recall roster
- Letters of appointment
- Intelligence mission statement
- Unit OIs

1.2.4. Written Instructions and Internal Reviews. Written instructions and periodic internal reviews are invaluable to the successful operation of a unit. They provide continuity during change of key personnel, guidance in quick reaction situations, aid in orienting and training new personnel, and assist in performing day-to-day operations.

1.2.5. Checklists, Directives, and Operating Instructions. Write checklists, directives, Unit OIs, etc., with care and attention to unit mission requirements, governing regulations, and Operations Plans

(OPLANs.) The final product should provide guidance that benefits the unit during in-garrison and wartime operations. The following list of items will assist in this task:

- Refer to AFI 33-360V1 for correct format of OIs.
- Write detailed instructions covering all critical tasks, but at a level that inexperienced individuals can understand.
- Checklists should be written as an abbreviation of the detailed instructions.
- As a minimum, formally review written instructions and checklists annually.
- In-processing checklist used by newcomers should identify written instructions that must be read. The completed checklist can be a permanent record of who has read the instructions.
- Policy letters are especially valuable to introduce newcomers to organizational norms.

1.2.6. Suspense Tracking and Internal Reviews. To deal with the sizeable workload and diverse tasking, it is important to periodically revisit the up-and-running programs to ensure they are still effective. Good review and suspense tracking programs are excellent tools to keep the organization on track.

1.2.6.1. Suspense Tracking System. Establishing a suspense tracking system is a wise idea. Consider setting aside a time each day to review suspenses. It is also important to monitor suspenses for outside tasking of your personnel. Look at the upcoming week's schedule, to include the aircrew and intelligence training schedule, verifications/certifications, and the like.

1.2.6.2. Unit Self-Assessment Program. The self-assessment program is a tool that can prevent problems during operations and inspections by identifying weak areas in time to fix them. Usually, the first priority at most units is aircrew-training programs in the squadrons. However, high marks in these areas do not necessarily guarantee a stellar inspection rating or smooth operations during wartime or contingency. A thorough self-assessment program can ensure all tasks are performed to standards. Although self-assessment programs must be tailored to each unit, the self-assessment checklists found on the AMC/IN's unclassified home page, under Unit Readiness, Unit Self-Assessment Checklist (**https://www.amcin.scott.af.mil/**), will provide a solid baseline to work from.

1.3. Personnel Management. People are our most important asset. Motivation and leadership are key to mission accomplishment. Assign them meaningful tasks, provide adequate time to complete the tasks, and allow them flexibility to develop innovative methods. Your people must feel they are part of the team with a stake in the outcome. The Intelligence Flight Commander (IFC)/OIC and Superintendent must strive to balance the workload among all personnel. This may require juggling of task assignments during periods of heavy tasking or short manning. Constantly monitor the status of projects, task loads, and suspense's within all subordinate functions. Manpower and personnel issues are continuing problems. Meet with your Commander and First Sergeant as soon as possible. Learn who, within the Military Personnel Flight (MPF), can help with critical personnel issues, such as classification and training, manning control, promotion and testing, and performance reporting.

1.3.1. Basic IFC/Superintendent Management Tasks. IFCs and their Superintendents must assume the key role in managing the assignment, classification, training, development, and evaluation of assigned people. This means ensuring deserving people are considered for awards, promotions, and special

assignments; and those performing below standards are appropriately trained and ensured opportunities to grow and develop. When necessary, counseling and disciplinary or administrative action should be taken. Basic knowledge of the manpower and personnel systems is a must.

1.3.2. Make a determined effort to know the personnel, their strengths, weaknesses, aspirations, and problems. Use this knowledge to achieve maximum productivity while heading off potential problems. Blend them into an efficient, cohesive team. Intelligence experience is often limited due to the age and rank of personnel. Additionally, some of the senior enlisted people will probably be cross-trainees with limited time in intelligence. These factors must be considered but are not insurmountable problems. Limited experience can be dealt with through a robust internal training program. Senior NCO cross-trainees with years of personnel training and supervision experience are tremendous assets.

1.3.3. Sensitive Compartmented Information (SCI) Billet Management. If the IFC is the unit SCI billet monitor, he will be dealing with the Management Engineering Team (MET) and the personnel and information security offices at the security forces squadron on Single Scope Background Investigations (SSBI) for personnel filling SCI positions.

1.3.4. The Unit Manning Document (UMD). The UMD reflects the total authorized manpower requirements, both funded and unfunded, for your organization. These authorizations are tasked against Unit Type Code (UTC) requirements. However, actual wartime requirements may exceed present manpower authorized in the UMD and UTCs. To revise the in-garrison UMD, contact the local manpower management office and HQ AMC for assistance.

1.3.5. The Unit Personnel Management Roster (UPMR). The UPMR lists the actual people assigned to the unit, as well as projected losses and gains. The information in the UPMR should match the manpower authorizations on the UMD. Periodically review the UPMR and UMD, compare them, and advise your unit-manning monitor of any discrepancies between the two.

1.3.6. Additional Duty Assignments. Additional duties can be a major concern to the intelligence flight/section. AFI 14-105, *Unit Intelligence Mission and Responsibilities,* specifically directs that intelligence personnel must not be assigned additional duties or details that would interfere with their contingency, wartime, or mobility tasking and intelligence support activities. AMC Sup1 to AFI 14-105 further prohibits intelligence personnel from being assigned additional duties as unit Personnel and Information Security Manager, Operations Security (OPSEC) or Communications Security (COMSEC) officials, military deception officer, Squadron Automated Data Processing Equipment (ADPE) monitor, or resource advisor. AMC Sup 1 also prohibits any 7-level enlisted member from being assigned any additional duties outside of intelligence. This does not preclude intelligence personnel from performing day-to-day additional duties that have no impact on deployment or employment operations. Make every effort to ensure individuals are not encumbered with additional duties that might detract from the performance of assigned intelligence tasks and responsibilities. Monitor additional duty assignments within intelligence units to ensure equitable distribution.

1.3.7. Awards Programs.

1.3.7.1. Individual Award Programs. Nominate personnel for all awards programs for which they are eligible and qualified. Use the AMC Intelligence Awards Program, the 12 Outstanding Airmen of the Year Program, and unit Airman, NCO, and Company Grade Officer of the Month and Quarter Programs to recognize superior performance. Do not assume a unit or personnel have no chance. The AMC individual award winners automatically compete at Air Force level.

1.3.7.2. Submission Guidelines. Submit intelligence personnel and unit nominations In Accordance With (IAW) AFI 36-2847, *Intelligence Awards*, and the Air Force Intelligence Awards Programs. Base and unit regulations will also contain guidance on awards programs.

1.3.7.3. Other Recognition Programs. Consider nominations for other recognition programs as well, such as the Outstanding Young Men and Women of the Year Awards Program (a civilian program) and the Federal Women of the Year Award Program.

1.3.7.4. Nomination Preparation. Junior officers and NCOs who are supervising for the first time should write award nominations on their people. This may mean more time will be spent by the IFC editing and rewriting nomination packages; however, teaching people to write effectively will be well worth the investment.

1.3.7.5. Success Tips. To obtain recognition for personnel, do the following:

- Search for opportunities for subordinates to excel. The IFC and superintendent should look at tasks they are personally performing with the idea of delegating the task to a junior officer or NCO. Encourage branch and section chiefs to do the same with their NCOs and airmen.

- Start preparing nomination packages well in advance of the suspense. Allow plenty of time for editing and polishing of each package. The significance of your nominee's accomplishments must be readily apparent to the selection board members.

1.4. Individual Mobilization Augmentee Program Management. The Air Force Reserve IMA program is one of the most flexible and responsive programs within the Air Force. IMAs bring valuable skills gained from active duty or civilian careers to their assigned units. The HQ AMC/IN Reserve Affairs Manager (RAM) administers the AMC IMA program.

1.4.1. Training Requirements. IMAs have two training requirements, fiscal year (FY) and Retention/ Retirement (R/R) year, which must be met in order to obtain a satisfactory (or "good") year. To ensure a satisfactory year for both FY and R/R participation, IMAs should schedule training during the longest period where their R/R year and the FY overlap.

1.4.1.1. R/R Participation. To earn a good year toward retirement, a member must earn a minimum of 50 points (includes 15 membership points) in their R/R year. If members fail to achieve a satisfactory year for two consecutive years, they will be placed in the inactive reserve.

1.4.1.2. FY Participation. IMAs must complete the minimum Inactive Duty Training (IDT) periods and Annual Training (AT) tour for their pay category from 1 October through 30 September. The AMC/IN RAM tracks all unexcused absences and notifies HQ ARPC of actions initiated to reassign unsatisfactory participants.

1.4.2. Annual Training (AT). Annual Training is the minimum period required to satisfy the annual training requirement. For Air Intelligence Agency (AIA) IMAs, the standard tour is 12 days, starting on Monday of the first week and ending on Friday of the second week. Weeks including holidays cannot be included in the tour except under special circumstances. Annual tours as long as 14 days can be approved with valid justification, subject to approval by the AMC/IN RAM and XOI/RE.

1.4.2.1. Requesting Annual Training (AT). Web Order Transaction System (WOTS) has replaced the AF Form 1289. WOTS is an automated training and school tour order request and tracking system. IMAs can request tours (after they have been approved by their supervisors) over the

internet through the ARPC homepage. (NOTE: You must enter the e-mail address of your supervisor and the RAM in the SUPERVISOR EMAIL ADDRESS block.) Requests will be automatically forwarded to the AMC Program Manager (PM) for approval, and then to ARPC for processing. WOTS is located on the ARPC homepage (**http://arpc.afrc.af.mil/**.) Access the Main Subjects area in the header and then proceed to WOTS. IMAs should receive a letter explaining their initial log-on information. There is also an IMA WOTS User Guide located at **http://arpc.afrc.af.mil/orders/WOTSIMA.DOC**. You may also contact ARPC at DSN 926-6261, ext. 8289 or (800) 525-0102.

1.4.2.2. Documenting Completion of AT Tour. Upon completing annual training, fill out blocks 38-46 of AF Form 938, *Request and Authorization for Active Duty Training/ Active Duty Tour*. Complete the End of Tour Report on the back of the orders within 10 days of tour completion. File a copy in the IMA Management Folder and send a copy to HQ AMC/IN RAM.

1.4.3. Inactive Duty Training (IDT). Inactive Duty Training consists of regularly scheduled training periods performed with their unit of attachment. AIA IMAs are in Category A and must complete 48 periods (24 days) of IDT each fiscal year.

1.4.3.1. Documenting IDT. Use the AF Form 40a, *Record of Individual Inactive Duty Training*, to report IDT points and to initiate action for pay and point entitlements. It should be certified and submitted immediately after completion of the training.

1.4.4. Active Duty Support (ADS). Active duty tours, less than 180 days, to support active or reserve units.

1.4.5. Active Duty for Training (ADT). ADTs are active duty tours used for training. They are intended to provide qualified personnel to fill the Armed Forces needs in time of war or national emergency.

1.4.6. Reserve Personnel Appropriation (RPA) Man-day Tours. Active duty tours intended to increase mobilization readiness or provide in-depth training. Tours include participation in joint training exercises, operational training, and attending conferences. Annual requests for man-days must be submitted through the functional manager prior to 15 March each year.

1.4.7. Military Personnel Appropriation (MPA) Man-day Tours. MPA man-days are authorized to support short-term needs of the active force. The HQ AMC/IN RAM manages the requirements for MPA tours. Pay and allowances are paid from military personnel appropriations, while units usually fund travel and per diem. Special tour requirements should be submitted to the HQ AMC/IN RAM by 15 March each year.

1.4.8. Reserve Support Team (RST). The RST exists to help the Air Reserve Component (ARC) insure the IMA program is integrated with the active duty units. The command's senior IMA is the RST team chief. Administrative responsibilities include OPR/EPRs, Quarterly IMA Participation Summary (QUIPS), weight management, ergometry, and ancillary training.

1.4.9. Reserve Pay Office (RPO). Each reserve member must designate a Reserve Pay Office (RPO) to process pay actions. The IMA should designate the RPO closest to their residence or training location. Reservists residing overseas will designate the Denver RPO for pay purposes. Clothing requests will by processed by the Denver RPO, regardless of category or location.

1.4.10. Schedules. Schedules must be coordinated to fulfill Fiscal Year and Retirement/ Retention year requirements. This must be a joint effort between the active duty supervisor and the IMA. IDT days can be combined or spread out through the year as needed, as long as requirements are met.

1.4.11. Telecommuting. Telecommuting is an authorized option for IMAs with a record of consistent satisfactory service. A request package must be completed IAW AFI 36-8002, *Telecommuting Guidelines For Air Force Reservists And Their Supervisors*, and forwarded to the HQ AMC/IN RAM for processing and final approval prior to starting any telecommute IDTs or tours.

1.4.12. IMA Management Folders. Supervisors of IMAs are required to establish IMA Management Folders. The folder should include the following sections:

Section 1 -	*Individual Mobilization Augmentee Wartime Job Description*
Section 2 -	*Assignment Orders*;
Section 3 -	AF Form 1561*, Individual Mobilization Augmentee Participation Schedule Worksheet* (ensure that this worksheet projects training for one year in advance);
Section 4 -	AF Form 40a's, *Record of Individual Inactive Duty Training*. Each completed form should be filed in this section;
Section 5 -	Annual tour orders, MPA/RPA orders, AF Form 1289 - *Request for Annual Tour* or RPA orders, (only if the annual tour is pending);
Section 6 -	AF Form 526, *ANG/USAFR Point Credit Summary*.

1.4.13. Requesting MPA/RPA tours outside of the Major Command (MAJCOM). To volunteer for tours outside of AMC, the IMA must first have written permission from the active duty supervisor. Once permission is obtained from the active duty supervisor, the IMA must send the AF Form 49 (Application for MPA Tours) to HQ AMC/INXU for MAJCOM approval and orders processing. The RAM will send the AF Form 49 and the supervisor's written approval to XOI/RE for approval and orders. Before supervisors grant approval for these tours, they must ensure that their IMA has already completed their IDT and annual tour requirements or that they are scheduled to complete them upon their return before the end of the FY.

1.4.14. Mobilization Procedures. HQ AMC RST will test mobilization recall procedures at least once a year. Therefore, it is imperative that the RST is able to communicate with the reserve member quickly. Please submit changes in home address and telephone numbers (home and civilian employment) in writing. Reservists should have a folder with all the documents required in the event of mobilization.

1.4.15. Military Standards. Reservists are required to comply with all Air Force Instructions.

1.4.16. Extension Course Institute (ECI) Courses.

1.4.16.1. Requests. Send requests for ECI courses through the Unit Training Manager to HQ ARPC/DAT. Reservists should submit a letter to HQ ARPC/DAT including name, grade, SSN, address, telephone number, name of the course, course number, and where they will be taking the End of Course (EOC) test. If they are not near an Air Force installation, they may arrange to take your test with an Army or Navy facility.

1.4.16.2. Requests can also be done on-line at **http://arpc.afrc.af.mil/dpat/PME** Spcld Courses.htm. Once on the ARPC homepage, click on Training and then military training. Then click on Correspondence Professional Military Education (PME) and Specialty Courses, and follow the on-screen directions from this point. Provide HQ AMC/IN RAM with a courtesy copy of all training requests for inclusion in your IMA folder.

Chapter 2

TRAINING

2.1. General. The purpose of internal training is to enhance and further expand professional knowledge and technical qualifications. Whether your shop consists of one or 30 people, you must have a training program. An effective training program requires comprehensive planning, careful scheduling, effective integration of internal and formal training, timely implementation, capable direction, skillful application, flexibility, and continual evaluation. You must carefully plan, select, and arrange your resources to best train your people. The quality of your planning will reflect in the quality of your results!

2.2. Career Field Education and Training Plan (CFETP). CFETP 1N0X1 is a comprehensive education and training document that identifies life cycle education/training requirements, training support resources, and minimum core task requirements for this specialty. The CFETP provides personnel a clear career path to success.

2.2.1. Using guidance provided in the CFETP will ensure you receive effective and efficient training at the appropriate point in your career. Use the CFETP to identify, plan, and conduct training commensurate with the overall goals of the plan.

2.2.2. The CFETP also:

2.2.2.1. Serves as a management tool to plan, manage, conduct, and evaluate a career field-training program. Also, it helps supervisors identify training at the appropriate points in an individual's career.

2.2.2.2. Identifies task and knowledge training requirements for each skill level in this specialty and recommends education/training throughout each phase of an individual's career.

2.2.2.3. Lists training courses available in the specialty, identifies sources of training, and the training delivery method.

2.2.2.4. Identifies major resource constraints that impact full implementation of the desired career field training process.

2.2.3. Use of the CFETP. All management levels will use the CFETP to ensure a comprehensive and cohesive training program is available and instituted for each individual in the enlisted career ladder. We highly recommend use of the CFETP in officer training as well.

2.2.4. Supervisors/Trainers Responsibilities (in coordination with unit training managers).

2.2.4.1. Develop, conduct, evaluate, and manage organizational training programs in accordance with the requirements set forth within CFETP 1N0X1 and per guidance contained in AFI 36-2201V3, Air Force Training Program On The Job Training Administration.

2.2.4.2. Identify, document, and report training shortfalls, through appropriate command channels, to MAJCOM functional managers.

2.2.4.3. Use the CFETP as a reference to support training.

2.2.5. Trainees' Responsibilities.

2.2.5.1. Complete the applicable mandatory training requirements specified within CFETP (identified as core tasks).

2.2.5.2. Periodically review the CFETP to ensure they are receiving the appropriate education/ training commensurate with their grade, skill level, and career path.

2.3. Developing an Internal Training Program. Your first step in developing an internal training program is to review the internal training requirements levied by the AMC supplement to AFI 14-105, *Unit Intelligence and Mission Responsibilities* and AMCI 14-107, *Command Intelligence Personnel Training Program*. Second, you must have 100 percent task coverage. This means identifying all tasks performed in your work center and specific individual positions. You must include contingency/wartime tasks, additional duties, and any mandatory requirement listed in AFMAN 36-2108, *Airman Classification*. Don't forget to include the applicable Special Interest Items.

2.3.1. Training Priorities. Once you determine the training requirements, you must prioritize those requirements. Requirements essential to your mission must receive top priority in your training plan. Certify trainees on mission essential activities first, and then proceed to other less essential duties.

2.3.2. Training Methods. After determining what your training needs are, next you must decide how to provide the training. We generally recommend the coach-pupil or demonstration-performance method; in other words "hands on, over-the-shoulder." The trainer demonstrates to the trainee the correct way of performing a specific task. The trainee then practices and performs the activity under controlled conditions and with close supervision until he/she is proficient. Keep in mind; the best training method may differ depending on the trainer, trainee, and task being trained. Flexibility is always a key concern.

2.3.3. Training Processes. The training process starts when you conduct an initial evaluation and orient a newly assigned individual. The new person may be fresh out of technical school or qualified in many tasks from previous assignments. Therefore, finding out where to start is key to saving time and effort.

2.3.4. Initial Orientation. During the initial orientation of the trainee you should, as a minimum:

-Outline the trainee's responsibilities/duties.

-Identify time spans and mandatory requirements the trainee must meet for position qualification and job certification.

-Determine career development course requirements (for enlisted, if entering upgrade training).

-Review the CFETP (for officers, you will have to establish a training folder). Consider all tasks performed in the duty position and compare the CFETP to overall work center requirements.

2.3.5. Initial Evaluation. During your initial evaluation of the individual's qualifications you should, as a minimum:

- Review past training and experience. Interview the individual and review the trainee's Job Qualification Standard (JQS)/CFETP to fully understand his/her background.
- Validate previously certified tasks. You must ensure the trainee's proficiency on all the tasks signed off. If you find the trainee cannot perform a signed off task, you must decertify them on the task and retrain the individual.
- Match duty position requirements to the qualifications of the trainee. Do not forget to consider any special contingency, wartime, recurring, or additional duty training the person may require.
- Determine the specific training the individual will need.

2.3.6. Conducting Training. Conduct evaluation and certification immediately upon completion of the training. Evaluation methods are dependent on the activities you want to measure. Evaluations can be oral, written, or practical application.

2.3.6.1. Oral Evaluations. Use oral evaluations throughout the training process or to supplement a practical evaluation. They are particularly useful to correct misconceptions on the spot and move the learning process in the right direction.

2.3.6.2. Written Examinations. Use written examinations to check the trainee's understanding of how to apply facts, principles, and procedures in performing a task.

2.3.6.3. Practical Evaluations. Practical evaluations are formal assessments of the trainee's ability to perform a task. The evaluator observes the trainee's performance and rates him/her on a pass/fail basis. To pass the evaluation, the trainee must demonstrate he/she is able to complete the task correctly in terms of procedures, timeliness, performance, and so forth, and the end product meets the mission objective.

2.3.7. Certifying Training. The last event in the training process is to document and certify the completion of training. Grant certification only if the trainee is able to perform the activity without assistance, appropriate to his/her skill level, unit, and mission. If this is not the case, do not certify the individual, as they need further training.

2.4. Formal Training.

2.4.1. Air Education and Training Command (AETC) Funded Training. Courses conducted by organizations and agencies (under AETC contract, Army, Navy, or other government agencies), whose primary mission is training or education, are AETC funded or eligible for AETC funding when funds are available (i.e., Survival Training (combat, water, and arctic) is AETC funded). Although eligible for AETC funding, it is the units' responsibility to budget for training to ensure funding is available during the FY you require the training. Courses conducted at the Intelligence Training Center, Goodfellow AFB TX, and the Joint Military Intelligence Training Center, Bolling AFB DC (National Intelligence Course, Indications and Warning Course, Counterterrorism Analyst Course, SCI Control Officers Course, and SCI Administrative Course, etc.) are eligible for AETC funds, if available.

2.4.2. Unit Funded Training. Units fund courses conducted by MAJCOMs and their operational units. Unit funded courses include:

-Air Mobility Warfare Center (AMWC), Ft Dix NJ
Intelligence Operations Orientation Course
Combat Air Tactics Course
Air Mobility Operations Course
-USAF Special Operations School, Hurlburt Field FL
Dynamics of International Terrorism
Latin American Orientation Course
Middle East Orientation
-Command and Control Warrior School (C2WS), Hurlburt Field FL
Air and Space Operations Center (AOC) Familiarization Course
AOC Initial Qualification Training
Intelligence, Surveillance, Reconnaissance (ISR) Officers Course
AOC Initial Qualification Training, Air Mobility Operations Course
AOC Initial Qualification Training, Personnel Recovery Course
-Advanced Airlift Tactics Training Center, St. Joseph MO
Practical Intelligence Course

2.4.2.1. Always forecast your formal training needs during the annual screening (May - September) based on the needs of your personnel and any projected gains. Forward both annual screening and out-of-cycle (identified after annual screening) requirements to HQ AMC/INXU. Early identification is critical to procuring the required number of seats and AETC funding.

2.5. Aircrew Intelligence Training (AIT). One of the most important functions of intelligence personnel during peacetime is the training of aircrews. AIT enhances AMC aircrew understanding of the threat and directly contributes to mission success and aircrew survival. Where possible, coordinate this training with unit tactics and life support. AIT is mandatory and is tracked by the Air Force Operations Resource Management System (AFORMS). Sign-in sheets should be provided to appropriate AFORMS personnel so aircrew records can be updated.

2.5.1. Establishing an AIT Program.

2.5.1.1. AFI 14-105, *Unit Intelligence Mission and Responsibilities,* requires all units to develop an annual AIT program. The AMC supplement to AFI 14-105 establishes specific AMC AIT requirements. It provides an AIT syllabus for each unit to use as an outline to build a program fitting its specific missions and responsibilities. To establish and provide a sound AIT program, you should acquire and maintain a high degree of knowledge of the subject matter and communicate your knowledge in a clear and comprehensive manner. Build your program around countries (and their associated threat systems) for which the potential for direct wing involvement is HIGH. Associate your training with real-world OPLAN/Operations Order (OPORD) tasking to demonstrate the relevance and realism of your training. Other units with similar aircraft/missions can be

excellent resources. Ask to review their AIT program, what innovative training aids do they use, what training philosophies they found successful, and what failures have they overcome. Always remember, if you use part of another unit's program, give credit where credit is due.

2.5.1.2. Give special attention to physical security. Ensure the facility is cleared for the security classification of the material you are covering. Also, ensure the facility is a comfortable environment for both you and the aircrew. Check with your local Security Forces Squadron (SFS) if you have questions regarding a secure area.

2.5.2. Keep AIT Interesting. Although AIT may save lives of aircrew, it is hard to convince the aircrews of AITs importance. Phrases such as "Who's going to shoot at us? We bring food and medicine to the needy" or "If they shoot us we are dead no matter what" or "We only fly outside threat areas" may imply that AIT is an unneeded training requirement. Keeping AIT interesting and related to current, real-world situations will help to battle these misconceptions and increase mission success.

2.5.2.1. If you review/teach a threat system your unit will not likely encounter, you immediately discredit the entire training session. Aircrews will question the instructor's credibility and understanding of the mission. The same can happen if the training is too technical. Keep the information at an easily understandable/useable level, i.e., threat ranges, firing doctrines, visual identification features, etc. If in doubt, ask a tactics representative for advice.

2.5.2.2. You will find the training is more effective and the aircrews are more responsive when the training is interactive. Give the audience a chance to participate and gain some recognition (e.g., "what's my line" or "your aircrews are in jeopardy".) Start a competition between flying squadrons tracking who has the best general knowledge. Post the results in a highly visible area to encourage friendly competition.

2.5.2.3. Know your material and project a strong and confident image. Allow constructive feedback and possible related topics or subjects to come up which may enhance the training. Try not to stray off course. If training sessions are lengthy, it may be a good idea to have more than one instructor available, if possible. Coordinate with your local life-support and tactics personnel. Let them lend their expertise to your training. Tag-team approaches to training (i.e., intel gives the threat and tactics briefs countermeasures) lend credibility and realism to AIT.

2.5.2.4. AIT Training Aids. Training aids can make or break your AIT presentation. Aircrews expect current, up-to-date aids that can compete with commercially available products; anything less will lose their attention and damage your credibility. Take advantage of the many new products that are available digitally. These digital images are more current than many of the images available hard copy, are easier to manipulate/label, and are readily incorporated into a PowerPoint/ Applix Graphics briefing. Remember to keep the training interesting by using many different types of aids; images, videos, interviews, debriefs, and examples of hard copy documents. Many of the products listed below are available from the 480th Intelligence Group (IG). If your unit does not have a current copy of the *Catalog of Recognition Materials,* a catalog is available on line at **http://intelink.ig480.langley.af.smil.mil**. The *Catalog of Recognition Materials* contains instructions to order the materials.

2.5.2.4.1. Recognition Guides, Journals, Books, and Manuals. Produced by various agencies, they are an excellent source for background information or pictures of weapon systems. Some source documents are:

-Jane's All the World Series Books

-International Defense Review

-British Recognition Journal

-Air Review

-Aviator's Recognition Manual

2.5.2.4.2. Recognition Posters. The 480 (IG) produces excellent posters. There are literally hundreds of different posters in circulation. There are wall posters that contain photos, line drawings, and textual data on the key recognition features of aircraft, ships, and ground equipment. These posters are large in size and are excellent for the walls in the intelligence facility or the squadron. These posters are available on SIPRNET at: **http://intelink.ig480.langley.af.smil.mil**.

2.5.2.4.3. Recognition Videos. The are also available at the 480 IG as well as other agencies. These videos present key recognition features associated with various weapon systems. They have a combination of freeze-motion shots of key features with action footage of weapon systems in operation (e.g., MIG-29 in flight) to provide a more realistic training environment for the aircrew and intel personnel. There are many different titles available covering aircraft, Anti-Aircraft Artillery (AAA), Surface-to-Air Missiles (SAMs), military studies, etc. These tapes can be a valuable tool to your recognition training program. They can also be used by the aircrew or intel personnel for self-study.

2.5.2.4.4. Commercial Products. There are a myriad of commercial recognition products available. Many are inexpensive and run on lower-end computer sites. They offer one-on-one, interactive recognition training. Although we do not discourage the use of these products, remember they are not DoD approved and cannot be part of your official recognition training.

2.5.3. Aircrew Testing. AIT is an annual training requirement as described in the Mission Design Series (MDS) specific AFI 11-2 training instructions. These instructions cover AMC airframes, as listed below. The purpose of testing is to collect valid metric data that can be used to assess the quality and effectiveness of training conducted. It's important to maintain good records to ensure the metric data is available and sufficient.

AFI 11-2 Training Instructions

AFI 11-2C-12V1, C-12 Aircrew Training

AFI 11-2C-130V1, C-130 Aircrew Training

AFI 11-2C-141V1, C-141 Aircrew Training

AFI 11-2C-17V1, C-17 Aircrew Training

AFI 11-2C-10V1, C-20 Aircrew Training

AFI 11-2C-21V1, C-21 Aircrew Training

AFI 11-2 Training Instructions

AFI 11-2C-5V1, C-5 Aircrew Training

AFI 11-2C-9V1, C-9 Aircrew Training

2.5.4. Supplemental Aircrew Training. Take advantage of recurring opportunities, such as operational briefings, flight meetings and scheduled down days. Briefings of 5-10 minutes on various subjects should be kept ready to present at any opportunity. Combine these short briefings when longer sessions are scheduled. If training sessions are lengthy ensure breaks are scheduled. Other supplemental training, such as threat of the day briefings, exercises, aircrew certification, etc., is highly recommended.

2.5.5. AIT Critique. Use critique sheets to find out the effectiveness of training. Remember aircrew input is very important; they are the customers. Use the critiques to tailor your training to meet the specific needs of the squadrons you support. Find out which training aids and instructional techniques the crews react best to, the quality of the instructor, and how the course could be manipulated to better prepare the crewmembers for their real-world missions. Never take the comments personally. Use this constructive criticism to improve your service to the customers. During training brief the improvements based on critique inputs so the crewmembers know their suggestions do not fall on deaf ears.

Sample Critique Sheet. Please help us improve your AIT by commenting on the following. Use the back of this sheet to elaborate on your comments.

1 = Poor 5 = Adequate 10 = Outstanding

1. Please rate the instructor.	**1 2 3 4 5 6 7 8 9 10**
2. Please rate the training aids.	**1 2 3 4 5 6 7 8 9 10**
3. Please rate each block of instruction for its usefulness to you.	
Hot Spots	**1 2 3 4 5 6 7 8 9 10**
Aircraft	**1 2 3 4 5 6 7 8 9 10**
SAMs	**1 2 3 4 5 6 7 8 9 10**
AAA	**1 2 3 4 5 6 7 8 9 10**
Naval Combatants	**1 2 3 4 5 6 7 8 9 10**
New or Upgraded Threats	**1 2 3 4 5 6 7 8 9 10**
Evasion and Recovery	**1 2 3 4 5 6 7 8 9 10**
Map Preparation and Symbology	**1 2 3 4 5 6 7 8 9 10**
Combat Intelligence Support	**1 2 3 4 5 6 7 8 9 10**

4. If you marked one of the above selections below a 5, please explain why.

_____

_____

_____

_____

5. Overall, how would you rate the course? 1 2 3 4 5 6 7 8 9 10

6. What could we do to improve AIT?

_____

_____

_____

_____

Optional: (required if you would like feedback on your inputs)

Name: _____

Unit: _____

Phone: _____

Chapter 3

INTELLIGENCE INFORMATION MANAGEMENT

3.1. General. DoD production agencies distribute documents directly to units with a valid DIA account number. If your unit mission or Area of Responsibility (AOR) changes, you'll need to update your Statement of Intelligence Interest (SII) in order to revalidate your DIA account number. Production agencies coordinate all distribution of intelligence documents with the United States Transportation Command (USTRANSCOM) Dissemination Program Manager (DPM), who in turn coordinates with the AMC Command Dissemination Manager (CDM). Also, keep in mind that management of intelligence information is only part of the total information management responsibility of an intelligence office. In fact, intelligence reference files and libraries must be accounted for in your office's official file plan. For the purpose of this pamphlet, we're going to focus on acquiring and maintaining intelligence information. Consult AFMAN 37-123*, Management of Records,* and Squadron/Group information managers for assistance with your overall information management program.

3.2. AMC Standard Intelligence Document List (SIDL). The AMC SIDL specifies the absolute minimum essential/mandatory documents to be maintained in unit libraries. Mandatory documents are those documents that all AMC units are required to maintain regardless of mission. These documents must be on hand (soft or hard copy) or on order unless HQ AMC/IN has specifically waived the requirement. Requests for waivers must be signed by the unit IFC and sent to HQ AMC/INXU for validation and coordination.

3.2.1. With the advent of the Internet and Intelink, many documents listed on the SIDL may be found on-line. You can find the SIDL on both the classified and unclassified AMC/IN home pages. The on-line SIDL contains embedded links to those on-line documents available over each network. These links and on-line availability are always subject to change. Each individual shares in the responsibility to report dead or bad links to the CDM. Finally, if you're going to rely on soft-copy documents, we strongly recommend you download them to local media to ensure availability even if connectivity fails.

3.2.2. HQ AMC reviews and updates the SIDL annually. As intelligence professionals doing the job every day, you're likely to find other documents and sources that will enhance your organization's effectiveness. We encourage you to submit suggestions for improvement of the AMC SIDL at any time. Please forward suggestions to HQ AMC/INXU.

3.3. Customer Requirements Registration System (CRRS).

3.3.1. Purpose and Methodology. CRRS data is used to establish unit requirements for finished intelligence documents. DIA uses CRRS to develop distribution lists for new or revised intelligence products. Units will not be included on document distribution lists without current CRRS data on file. To satisfy this critical requirement, each unit with a DIA document account completes a computer-based worksheet that includes:

- Unit designator
- Mission statement
- DSN and commercial voice and fax numbers

- Unit area of interest by geographic and subject category
- Desired media and classification of intelligence products (CD-ROM, hardcopy, etc.)
- Unit points of contact

3.3.2. Updating and Maintaining CRRS Data. CRRS data is updated via DIA's Joint Dissemination System (JDS). Once your unit's DIA account has been established, JDS allows you to maintain your account directly from your unit. With JDS, you can access your own account to modify/update unit information, document requirements, and other CRRS data. JDS is accessible via the AMC/IN Intelink-S homepage by clicking on the "Support" tab, then scrolling down to the tab "AMC Document Dissemination Products" located under the "AMC Unit Support Products" heading. Remember that CRRS and JDS only establish requirements for automatic distribution of new or revised finished intelligence products. To receive documents that have already been produced and for one time issue, the document order process must be initiated.

3.4. Document Request Process. There are two forms used for requesting one-time distribution of finished intelligence documents. DD Form 1142*, Inter-Agency Document Request*, is used to request a single document. DD Form 1142-1 is used to request multiple documents on a single form. The completed DD Form 1142/1142-1 is sent to the AMC CDM. After validating the request, the AMC CDM forwards it to USTRANSCOM DPM for action. Again, these requests are for one-time distribution and do not affect recurring distribution.

3.4.1. Unit Actions.

3.4.1.1. Upon determining the need for a specific document, unit personnel complete DD Form 1142/1142-1.

3.4.1.2. Forward the 1142/1142-1 to the AMC CDM (HQ AMC/INXU). This process can be accomplished via the following means:

- E-Mail. Attach completed soft copy 1142/1142-1 to email and send to the AMC CDM at **mailto:INXU-all@amc.af.smil.mil**. Alternate method is to send regular email with all data that would normally be entered into an 1142. Either email option is the preferred method, as it provides rapid, accountable transmission in a form that is easily forwarded once validated.

- Fax. Send a completed hard copy to the CDM via fax. Initial transmission may even be quicker than e-mail; however, because the CDM will have to transcribe to soft copy, delays can be encountered. As with any fax transaction, it's a good idea to follow up with a phone call to make sure the fax was received and readable.

- Snail Mail. While extremely reliable, this means is very slow. However, it's well suited to routine requests when a quick turn-around is not required.

- Voice. This method should be reserved for time critical requests or when no other means is available. While as fast or faster than any other means, there's always a potential for transcription errors. Always follow up a voice request with one of the more accountable means above after time and/or connectivity become available.

3.4.1.3. Establish Suspense. The requesting unit establishes a desired date for receipt of the documents. If not received by that date, initiate follow-up with the AMC CDM. For routine requests,

suspense of 45 days is reasonable. For more time sensitive requests, suspense should be established and agreed to by the requesting unit and the CDM.

3.4.2. CDM Actions. Upon receipt, AMC/INXU validates your request. In many cases, INXU can locate and order the document for you. In other instances, the request may be referred to the USTRANSCOM DPM for assistance. Either way, you will be advised of the status of your request and an estimated delivery date.

3.5. Reference Library Structure. Once documents are received, they must be filed in a manner that makes them readily available. The key is to keep it simple. A recommended file system is to use the Intelligence Function Code (IFC) and geopolitical area codes. Both of these coding systems are understood and used throughout the intelligence community. Two examples of document file numbers using this system are provided below.

3.5.1. 1300-CU-01

- 1300 is the IFC for Air Forces, general information.
- CU is the country code for Cuba.
- 01 is simply the first document filed on that subject.

3.5.2. 1330-AJ-03

- 1330 is the IFC for Air Forces, Unit-Level Force Capabilities, Doctrine, and Structure.
- AJ is the country code for Azerbaijan.
- 03 means this is the third document filed concerning this subject and geographic region.

3.5.3. This simple filing method can be used worldwide and if adopted by all units would greatly simplify transitions. Personnel deploying to work with other units would already be familiar with the filing system. When transferring to another assignment, valuable spin up time would not be used on learning a unique filing system. A complete list of IFCs and geopolitical Area Codes is available in DOD-0000-151A-95, *Department of Defense Intelligence Production Program: Production Responsibilities*.

3.6. Requests for Information and Imagery (RFI).

3.6.1. Refer to AMC Instruction 14-103, *Procedures for Requesting Intelligence Information and Imagery,* for specific RFI guidance and responsibilities.

3.6.2. The intent of the RFI system is to provide an avenue for intelligence units to gain new information/imagery or to supplement information/imagery already known. AMC/INO is the focal point for substantive operational intelligence information and imagery. Before submitting an RFI, units should exhaust all local holdings and resources (INTELINK-S, library, etc.).

3.6.3. RFIs are submitted using the online form found on AMC/IN's SIPRNET homepage, under "On Line Forms", then "General Intelligence Forms" (**http://www.amcin.scott.af.smil.mil**). Other means, such as secure phone or fax, should only be used when a unit does not have SIPRNET access or the RFI is time critical (needing immediate attention) or time sensitive (needing response within 48 hours). If you use the secure phone, always follow up with hard/electronic copy correspondence as

soon as possible. Improper planning is not an excuse for submitting a time sensitive or time critical RFI.

3.6.4. All RFIs require a suspense date. The familiar jargon, “ASAP”, does not define any duration of time. Know your briefing requirements and file your RFIs as early as possible. A justification for the requirement is also necessary for processing. This will assist the RFI Manager in understanding the request and assist in prioritizing it. The more time you provide INO, the better product you will receive. When submitting an RFI, be as specific as possible. Do not ask broad-based questions such as "What is going on in country X?" or "Give me a current situation update." Ask the specific questions you do not have answers to, such as "What is the current total number of American Citizens (AMCIT) in country X?" or "Are there any terrorist threat to AMC assets in city X?"

3.6.5. AMC’s RFI process includes the following major steps:

- A unit submits an RFI via AMC/IN’s homepage.

- AMC/INOF reviews the RFI, determines its validity, clarifies it when necessary, and decides if the RFI can be answered at the AMC level. If there are problems with the RFI, the unit will be contacted so that the RFI can either be retracted or corrected as necessary.

- If the RFI can be answered, INOP either answers the RFI or passes it to INOA so that it can be assigned to the appropriate analyst. The individual assigned the RFI provides an answer via the online system. If the answer requires a document or image, the online system will still be used to respond to the RFI but the appropriate file will be e-mailed separately to the unit (the online system does not currently support attaching files to responses).

- RFIs that cannot be answered by AMC/INO are reviewed by AMC’s validation officer for submission to JICTRANS via the Community On-Line System for End Users and Managers (COLISEUM). Units will be notified if their request is entered into COLISEUM.

- JICTRANS validates the RFI and forwards it to the appropriate production center (NMJIC, NAIC, etc.).

- Response to the RFI will pass from the production center through JICTRANS to AMC/INO. This response will be transferred to AMC/IN’s RFI system so that the unit can be given the answer.

- When the unit is satisfied with the answer, the RFI is closed.

3.6.6. For units deployed or CHOP’d to a Combatant Command, AMC units need to utilize that Command’s RFI procedures for information and imagery.

Chapter 4

ANALYSIS AND ASSESSMENT

4.1. General. Air Force Doctrine Document (AFDD) 2.52, *Intelligence, Surveillance, and Reconnaissance Operations*, defines intelligence as:"the product resulting from the collection, integration, analysis, evaluation, and interpretation of available information concerning foreign countries, or areas; it is the information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. More specifically, the Air Force understands that intelligence efforts will primarily focus on foreign military capabilities; political groups; political, social, and technological developments; or certain geographic regions."The most important function of the unit intelligence flight is to analyze intelligence information in terms of its importance to, and impact on, the unit and mission. To be completely successful, intelligence personnel must know the customer they're supporting. They must establish a firm baseline of intelligence information from which to conduct analyses and make assessments. Finally, they need a well-understood, established process to use in assembling their efforts into a useable product.

4.2. Know the Customer. You need to know the customers who will be using your products and services. A solid knowledge of the customer will help to ensure your efforts are focused on the problems that need your utmost attention.

4.2.1. Commander. The commander is the prime customer and provides the overall direction to be followed in achieving mission objectives. As the person responsible for the long-range pursuit of a desired end state, the commander's focus will be general and more strategic in nature than that of a mission planner or crewmember. You'll need to know how he thinks, what information he typically has the highest demand for, and tailor your support accordingly.

4.2.2. Operators. In addition to operational information, you should learn as much as possible about the background of your crews and their airframes, including previous intelligence training they have received. Second Lieutenants just out of pilot training may need a great deal more support from intelligence. Most importantly, find out which threats concern, or should concern, them the most. Spend the most time researching and training on those threats. Ask the customers what they need and develop the program accordingly. Ensure they know just what you can contribute to the mission planning process. Fly with your aircrew often. This will let you see what they see and hear what they hear. Your understanding of the airframe and how the aircrew works together will allow you to better tailor your intelligence support to their needs. Flying on training missions in CONUS and flying when forward deployed is essential to being a better intelligence professional. Should the opportunity arise, fly on other platforms as well to increase your knowledge of operations in the Air Force. This is easily done by networking with other intelligence personnel in units that are deployed in your same area.

4.2.3. Other Base Agencies. Other organizations on base need your support as well. The needs of these organizations may be much different from those of the operator. Maintenance forces will need to know how much time they'll have prior to an attack once notified that it's coming. Security forces will want to know the capabilities of enemy special forces that may operate in the area and classic "ground perspective" intelligence issues. Readiness personnel may need to know about enemy chemical and conventional munitions. Establish a good working relationship with the Office of Special Investigations (OSI), as they can be an excellent source of terrorism and counterintelligence information. Conversely, you may have information that OSI needs. Your job is to support the whole unit, including

operations, medical, services, and logistics elements. As with other customers, ask them what they need and be prepared to prioritize requirements.

4.3. Order-of-Battle (OB) and Situation Displays. OB and situation displays form the foundation upon which an intelligence baseline is built. The purpose of these displays is to provide commanders, crews, and intelligence personnel with a visual portrayal to support briefings, serve as decision aids, assist in mission planning, and for use as an analytical intelligence tool. It is important to realize that there are many different versions of OBs available, with varying degrees of accuracy. It is crucial to find out which is the definitive OB, as established by the Combatant Commander. There are a variety of methods available to build and maintain OB and situation displays. They may be computer generated and projected on a screen, with incoming updates automatically plotted and displayed in near real time. They may be paper chart-based wall displays with clear plastic overlays and updates manually plotted by intelligence personnel from hard copy messages and reports. The particular method used is nearly irrelevant, provided it meets the needs of the unit and is readily available under any circumstance. The depth of detail presented on such displays is entirely dependent upon unit and mission requirements. While there are some similarities and overlap in function between OB and situation displays, there are also some significant differences. Unique aspects of each are discussed separately.

4.3.1. Significant Situation and Order-of-Battle Documents. Standard symbology used and understood by land, sea, and air forces is an essential ingredient to joint war fighting in general, and total battle space management in particular. Situation and command data must be seamlessly exchanged across services and disciplines, regardless of the specific C4I systems being used. Even on manually plotted charts, the symbology used must immediately and accurately convey the intended meaning to all that view it. The following documents provide guidance and tools to standardize symbology and OB displays.

4.3.1.1. MIL-STD-2525B *Department of Defense Interface Standard-Common Warfighting Symbology*. All Departments and Agencies of the Department of Defense (DoD) have approved this standard for use. The standard is designed to eliminate conflicts within various symbol sets and to bring a core set of common warfighting symbology under one DoD standard. MIL-STD-2525B is designed to equip DoD with a standard solution that provides sets of C4I symbols, a coding scheme for symbol automation and information transfer, an information hierarchy and taxonomy, and technical details to support systems. MIL-STD-2525B is the primary reference that DoD uses to standardize warfighting symbology. NOTE: This is a standard to which automated display symbology must conform.

4.3.1.2. Field Manual (FM) 101-5-1, *Operational Terms and Graphics*. This manual sets forth doctrine for the United States Army and Marine Corps in the use of land-based warfighting symbology. It serves as the primary guide for practical, unit-level, plotting and display symbology. It fully agrees with and supports MIL-STD-2525B. NOTE: This is the manual AMC unit intelligence elements use to plot displays.

4.3.2. OB Displays. OB displays focus on depicting the enemy's strength, status, and location. These displays are useful as an indications and warning tool prior to hostilities breaking out. They readily show current strength of forces and assets at specific locations. Fluctuations in strength always mean something (deployment for training, unit rotations, forward deployment for offensive or defensive operations, etc.) You acquire baseline and updated OB data from the appropriate theater analysis cen-

ters (Joint Intelligence Center (JIC), Joint Analysis Center (JAC), Regional Intelligence Center, etc.) JIC and JAC OB products are linked to the AMC SIPRNET homepage under "Intel Products."

4.3.2.1. Ground Order-of-Battle (GOB). GOB depicts the enemy's ground forces. Plot the entire GOB to the maximum level of detail possible/practical. The minimum satisfactory level of detail for AMC units is to the division level. Learn to use control measure and boundary markings as detailed in FM 101-5-1, Chapter 3. Plot units and equipment as appropriate, using symbology in FM 101-5-1, Chapters 4 and 5. When plotting ground forces, pay particular attention to air defense assets associated with ground units. It's absolutely critical to know the air defense systems that deploy with ground forces, the echelon levels they deploy at, how many deploy, and general deployment patterns used. This will require research well in advance of plotting the actual displays.

4.3.2.2. Naval Order-of-Battle (NOB). The naval element is often the most overlooked by Air Force units. Modern naval vessels often carry a massive array of highly lethal air defense assets. Research and plot NOB in as much detail as possible/practical and with due regard to unit location and operating areas. Plot primary, alternate, and dispersed bases of operation noting in-port vessel strength. For vessels deployed out of port, plot location and time of latest contact, as well as direction and speed of travel. When plotting warfare groupings, such as Surface Action Groups, Carrier Battle Groups, Convoys, etc., it's critical to know the types of vessels in the groupings. While not necessarily appropriate for plotting on the OB display, all intelligence personnel must be able to discuss shipborne air defense assets, including detection, tracking, and lethal engagement ranges.

4.3.2.3. Electronic Order-of-Battle (EOB). A natural tendency is to focus on the actual threat systems that can destroy our aircraft; however, most of these systems pose little or no threat without the associated detection, tracking, and guidance capabilities provided by electronic systems. These electronic systems are at the heart of most threat systems' capabilities. EOB displays should include passive detection systems (Radio Frequency (RF) monitoring sites, listening-posts, and even visual lookout posts) as well as radar systems. Correlate specific radar sites to function (surface search, air search, acquisition, height finder, target tracking, terrestial emitter, etc.) and to associated threats (surface to air missile sites/launchers, AAA emplacements, SATCOM jammer, etc.). When plotting EOB, ensure that each system plotted is easily and quickly referenced back to its function and associated threat. Graphically depict detection rings scaled to specific, appropriate aircraft altitudes. For low-level missions, terrain-masking envelopes should be analyzed and plotted when the mission warrants. If/when possible, plot lines of communication between sites and their direction/control centers. The key in the initial stages is to plot all EOB, as later mission planning and threat analysis efforts will depend on having all pertinent data.

4.3.2.4. Air Order-of-Battle (AOB). AOB is plotted as a function of an operating base and the associated units and aircraft assigned to or operating from that base. As used here, base can refer to any suitable operating location, including main operating bases, forward operating locations, austere operating locations, possibly even unimproved clearings. Suitable operating locations may vary widely depending upon the airframe. An important aspect of plotting AOB is to denote specific airframes and variants, currently known and/or assessed numbers, and assessed readiness status of aircraft present. While not necessarily appropriate for display on the actual OB chart, all intelligence personnel must be able to readily identify and discuss air-to-air and air-to-ground mission capabilities and munitions associated with the aircraft.

4.3.2.5. Defensive Missile Order-Of-Battle (DMOB). The enemy's DMOB may consist of a mix of fixed and mobile Surface-to-Air Missile (SAM) systems. Fixed sites, are easily identified, plotted, and monitored. The more mobile a system is, the more difficult it will be to maintain a current OB. Certain highly mobile SAM systems are normally assigned to ground-maneuver units, and should be accounted for in the GOB. Man portable SAMs can be anywhere and prove most difficult to accurately locate and track. While the effort may prove difficult, the mere purpose of these weapons, having been designed strictly to shoot down our aircraft, demands priority effort.

4.3.2.6. Anti-Aircraft Artillery Order-Of-Battle (AAAOB). Normally, AAA is associated directly to ground-maneuver units; however, these weapons have been deployed and employed in every manner imaginable, including point defense of strategic targets. The mobility of these systems makes it very difficult to maintain an accurate OB. However, heavy fixed emplacements should be plotted and tracked as appropriate. Sightings of AAA fire in/around mission areas should always be plotted and briefed until the threat is sufficiently mitigated. While the best source of baseline data will still be the theater JIC/JAC, Mission Reports (MISREPs) will often provide the most current information available. Though information reported in a MISREP is not evaluated, finished intelligence, never discount the value of information provided by people who had "eyes-on."

4.3.3. Situation Displays. If properly constructed and maintained, a situation display is the most critical analytical tool at your disposal. A situation display depicts an entire battlespace. It consists of elements of all OB displays scaled to a specific level of detail and purpose. It provides a graphical representation of the enemy situation, including Forward Line of Own Troops (FLOT), Forward Edge of the Battle Area (FEBA), axes of advance, troop locations and movements, etc. Additionally, a situation display includes friendly force information, including Blue Force OB, Minimum Risk Routes (MRRs), missile engagement zones, areas significant for Evasion and Recovery (E&R) and Combat Search and Rescue (CSAR), and much more. Significant event data, such as aircraft shoot-down locations, force build-ups, rear area attacks, major engagements, etc., are also tracked on the situation display. The tremendous amount of data plotted will normally require several different "layers" of display capability (overlays) so particular aspects can be temporarily removed, moved to the back, or brought to the front as needed. To be of any real use, the situation display must be continuously reviewed and updated with current information. Finally, as with any intelligence display, overall classification, current as of date/time, and a detailed legend must accompany the chart.

4.3.4. The Intelligence Baseline. An intelligence baseline is established when all previously researched, finished intelligence (capability studies, historical analyses, etc.) is combined with the current adversary OB and situation information. The end result is a fused, coherent, graphical representation depicting the adversary's current situation. It's absolutely imperative that this baseline be completely accurate, as comprehensive as possible, and maintained constantly. Every primary function of intelligence that must follow depends on the accuracy and completeness of the intelligence baseline. The next critical process is to determine what the adversary is going to do, where he's going to do it, and how he will attempt it. This is where Intelligence Preparation of the Battlespace takes over.

4.4. Intelligence Preparation of the Battlespace (IPB). Intelligence personnel are accustomed to discussing "intelligence analysis;" however, the literal definition of the word "analysis" is to "separate a whole into its component parts." Within the classic model of the intelligence production cycle, analysis is merely one process within the production phase. In the context of unit intelligence operations, simply offering "analysis" is not nearly enough. Your customers need a full spectrum "picture" of the entire battle

situation on which to base their decisions. When adapted to the aerospace environment, IPB is well suited to this purpose. While a comprehensive dissertation on IPB exceeds the purpose of this publication, a discussion of its fundamentals should highlight the importance of this concept.

4.4.1. The US Army has developed and refined the IPB concept to an institutionalized process well suited to its operational ground environment. As an "aerospace force," the Air Force must tailor the Army's primarily two-dimensional, geographically based concept into a full spectrum process. To better understand IPB and develop a working approach to it, two documents should be printed and studied in depth. Army Field Manual 34-130, *Intelligence Preparation of the Battlefield*, is available from the Army Publications Homepage (**http://www.adtdl.army.mil/atdls.htm**) on the unclassified internet and provides a critical baseline to this proven concept. For additional information on Predictive Battlespace Awareness (PBA) and IPB, see AF Pamphlet (AFPAM) 14-118, *Aerospace Intelligence Preparation of the Battlespace*, and Joint Pub 2-01.3, *Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace*.

4.4.2. IPB is a systematic, continuous process of analyzing the threat and environment in a specific battlespace. It enables the commander, staff, and mission crews to visualize the full spectrum of the adversary's capabilities, limitations, Centers of Gravity (COGs), and Courses of Action (COAs) across all dimensions of the battlespace. IPB is not solely concerned with the adversary, but also the environment of the battlespace and its affects on both hostile and friendly forces. As a process it offers various products. For unit-level operations, the key product is an intelligence estimate tailored to a specific mission problem set. There are four interrelated and continuous steps in the IPB process. These steps are cyclical and must be conducted before, during, and after every operational evolution.

4.4.2.1. Step 1 -- Define the Battlespace Environment. Step one defines the limits of the battlespace. For each operation planned, the Operational Area (OA), Area of Interest (AI), and mission must be determined. These three elements define the battlespace for a particular IPB iteration. For our purposes, the OA may be a deployment location, mission objective area, or refueling orbit. The AI is generally larger than the OA, and includes areas adjacent to, above, or below the OA that possess environmental factors or contain enemy forces capable of impacting operations. The intent of this step is to narrow down those areas the mission or unit will operate in to allow a focused assessment of issues with a real potential to affect the specific mission or unit.

4.4.2.1.1. The mission is typically defined by orders received (deployment orders, Air Tasking Order (ATO)). Determining the OA and AI flow is normally a natural function once the tasked mission is defined. Once the OA and AI have been defined, a review of currently held, baseline information must be conducted. This review should highlight gaps in required battlespace environmental and adversary data. These gaps are developed into information requirements that are further researched and satisfied locally, or up-channeled for HHQ assistance.

4.4.2.1.2. Step one should yield three final results. First, a preliminary set of priority intelligence requirements delineating the scope and detail required for the mission being planned should be documented. Second, significant battlespace characteristics affecting the mission should be identified and documented. Finally, gaps in available intelligence and information should be identified and prioritized for resolution.

4.4.2.1.3. Perhaps the following example will put step one into perspective. We're engaged in strike operations deep within a hostile nation. When the next ATO drops, your unit is tasked to establish a refueling orbit 60 NM north of the northern border of that nation. The OA is the

orbit area. The AI includes the route to/from the orbit area, and any surrounding areas that contain hostile forces with a potential to impact the mission (any SA-5s out there?) You must narrow your focus to the orbit area to determine if the mission can be conducted as tasked or if threats are high enough to require mitigation. While looking at the route in/out, you must determine if there are any threats along the way to warrant concern. Other information required by the mission planner may include weather forecasts for the area and time of the mission, objective of the mission (required fuel load), and inherent or imposed limitations on any of these considerations. Any information required but not available becomes a gap for which a requirement must be initiated.

4.4.2.2. Step Two – Describe the Battlespace's Effects. The purpose of step two is to determine how the battlespace defined in step one affects (positively or negatively) friendly and hostile operations. Again, more than just pure intelligence data is required for this step. Weather is just one other such data source. This step seeks to find any/all factors, geographical, environmental, political, etc, that can aid or limit options available to either friendly or hostile forces in developing COAs. It also seeks to determine specific impacts the battlespace imposes upon both friendly and hostile weapons systems. Continuing the refueling orbit example, if there are SA-5's within range of the orbit area, does the orbit altitude and range put the mission below effective detection range? Is weather offering a positive effect on the mission? On the enemy? Is the political environment right to encourage the enemy to attempt a High Value Airborne Asset (HVAA) attack over its neighbor's territory?

4.4.2.3. Step Three – Evaluate the Adversary. The purpose of this step is to determine the adversary's COGs, capabilities, doctrine, and applicable tactics, techniques, and procedures. While much of step three is geared towards developing and selecting targets, which is not much of a player for AMC mission's, the fundamental focus of understanding the enemy's capabilities and limitations is quite important. In Air Force IPB, step three consists of 4 elements: Analyzing and identifying enemy COGs; Creating and updating threat models; Determining the current adversary situation; Identifying adversary capabilities.

4.4.2.3.1. Analyze COGs. COG analysis seeks to identify those elements from which the adversary derives freedom of action, physical strength, and/or the will to fight. Those COGs determined to be truly critical to the enemy's strategy and ability to continue the fight tend to become priority objectives of the targeting process.

4.4.2.3.2. Create and Update Threat Models. Threat models describe and graphically portray threat tactics and employment options. A threat model could be as simple as a plotted SAM site with an outer range ring depicting maximum effective range, and an inner ring depicting maximum observed engagement range. The objective is to graphically depict the enemy's capability and demonstrated or assessed preferences for employing that capability. This process is necessarily continuous. As information is received that alters any aspect of the adversary's threat capability and/or intention, associated threat models must be reviewed, analyzed, and updated.

4.4.2.3.3. Determine Current Adversary Situation. This is an intelligence assessment of the enemy's current state. It includes a detailed analysis of relevant OB data, including force strength, composition, positions, and observed Tactics, Techniques and Procedures (TTP). The adversary's situation, including occupied terrain, forces available, logistics feasibility, communications effectiveness, morale, etc., when combined, creates a situation that opposing

forces must contend with. Only by understanding this situation, can an accurate estimate of his real capabilities be developed.

4.4.2.3.4. Identify Adversary Capabilities. To determine real capabilities requires a quantitative assessment of OB combined with a qualitative assessment of the enemy's readiness, training, and effectiveness. During this phase, all available information developed from all previous steps is rolled into an assessment of the adversary's capabilities. The key to a useable assessment is to establish a detailed description of the enemy's real capabilities. These capabilities are the result of identifying ideal capabilities, then applying mitigating factors that add to or detract from those ideal limits. When used during the target development process, this step finalizes the effort to determine which COGs provide the most impact when effectively struck. For our purposes, it identifies the highest threat areas that our mission planning efforts must either avoid or otherwise call for mitigation against.

4.4.2.4. Step Four – Determine Adversary Courses of Actions. Step four integrates the previous steps into a meaningful conclusion. It identifies, develops, and prioritizes COAs consistent with the COGs developed in step three. It also identifies the adversary's doctrine and assessed political/military objectives. As with step three, this step is also "targeting-centric," but still has applicability if applied properly to mobility air force operations.

4.4.2.4.1. In the overall Air Force IPB process, there are six sub-steps included in step four, each of which constitutes its final products. They are:

- Identify the adversary's likely objectives and desired end state.
- Evaluate and prioritize adversary COAs and their associated strategic, operational, or tactical COGs.
- Explicitly identify threat assumptions.
- Identify targets valuable to the adversary in executing probable COAs and nominate for attack those targets that will achieve the chosen friendly COA and objectives.
- Identify collection requirements that monitor significant battlespace characteristics, provide indications of which COA the enemy has selected, and assist the command in assessing his operational effectiveness
- Produce decision support products that ensure intelligence sensors and producers are arrayed to collect, process, exploit, and disseminate the right data at the right time to support key operations decisions.

4.4.2.4.2. To put step four into the mobility air force perspective, some interpretations of the final results are required. The intended audience and its focus will also affect these interpretations. For example, when used to support mission planning, each of the six products of step four must be narrowed in scope to the specific mission being planned. When working with the on-site Threat Working Group (TWG), a somewhat higher, longer-term view is needed, yet the focus should remain narrowed sufficiently to highlight the factors that may/will affect the deployed location. When briefing the Battle Staff, an even higher level view must be taken, broadening out to include yet a longer range look at what the enemy can be expected to attempt in the next 24, 48, and 72 hours or more. The end result must clearly indicate how those attempts will impact the unit's ability to accomplish assigned missions.

4.5. The Intelligence Estimate. The results of the IPB process culminate in the development of the intelligence estimate. As with the entire IPB process, an intelligence estimate must be developed at all levels and phases of an operation. This includes prior to a crisis, through the development of a crisis, through the onset and conduct of hostile operations, and following through the conclusion of hostilities and return to peace. Also, the intelligence estimate must be completely scaleable to the particular mission, operation, or problem set being worked. At the flying end of operations, it must be developed prior to operational mission planning, and must subsequently and continuously be updated and revised throughout the life of an operation, contingency, or other situation. While the actual form and media must be whatever is most appropriate and most useable by the customer, in its most basic form, the intelligence estimate is a written document with five paragraphs.

4.5.1. Paragraph 1 – Mission. This is simply a restatement of the particular mission the estimate is developed to support. The mission may be that of an entire force, the whole unit, or of a single sortie aircraft and crew.

4.5.2. Paragraph 2 – Area of Operations. This paragraph describes the area of operations as defined in Step Two of the IPB process. It must also define how the battlespace environment affects the enemy and friendly forces.

4.5.3. Paragraph 3 – Enemy Situation. This paragraph is derived from step three of the IPB process. It clearly defines and describes the enemy's current situation in terms of facts (exact location, known operating envelope, known limitations, previous expenditures, etc.) and assumptions (analyzed impact of weather, attrition, psychological affects, etc.).

4.5.4. Paragraph 4 – Enemy Capabilities. This is a listing and discussion, derived from step four of the IPB process, of the COAs available to the enemy. There should always be at least two COAs (generally more) for any situation. The enemy's "most likely" COA, and the "most dangerous" COA. This combination gives the commander/planner a realistic view of what to expect, while also showing the worst case that must be anticipated.

4.5.5. Paragraph 5 – Conclusions. This paragraph is derived from the evaluations made during the IPB process. It is a summary of the effects of the battlespace on both friendly and enemy COAs, list probable COAs in order of probability, and list the threat's exploitable weaknesses.

4.6. Sources/Aids. There are a number of sources and methods of drawing assistance available. Some of these are discussed below.

4.6.1. Finished Intelligence Products. As discussed in **Chapter 3**, finished intelligence is available via hard-copy documents and other products. Many products are available directly from the producer and/or DIA via SIPRNET/Intelink-S. Other products are only available in specified forms. Get familiar with what's available and how to receive it before you need it. These products are crucial to development of the baseline upon which everything is must be built.

4.6.2. Near-Real-Time (NRT) Intelligence. Several avenues exist for receipt of NRT intelligence. This data provides the most current, timely updates available. Some NRT data is available via SIPRNET/Intelink-S. Some can be accessed via a dial-up to the AMC/IN Servers (TRAP Feed). With Tactical Receive Equipment (TRE), NRT intelligence data is available nearly non-stop, and with little to no external interference.

4.6.3. Personal Computer Integrated Imagery and Intelligence (PC-I3). PC-I3 is a system that can be used to provide necessary intelligence and mission planning data to wings and squadrons via

web-based technology. The PC-I3 hardware configuration is based on a Windows NT architecture using PC workstations. It includes a web-based search engine to query databases (i.e., IPL, MIDB, 5D, etc) and to retrieve data supporting various unit-level intelligence functions (Order-of-Battle Display, ATO/Airspace Control Order (ACO) Breakout, Mission Planning Support, Combat Mission Folder Development, Briefing and Reporting). For PC-I3 documentation, visit ACC's SIPRNET site at **https://in.acc.af.smil.mil/**.

4.6.4. Force Protection/Threat Working Group (TWG). The HQ AMC TWG is the Command focal point for coordinated threat analysis and FP recommendations for all AMC operations.

4.6.4.1. Senior leaders from HQ AMC intelligence, counter-intelligence, security forces, AFOSI, medical and operations meet daily in the AMC TWG to assess current and potential threats affecting AMC planning and operations. These time-sensitive, coordinated threat analyses and FP recommendations are based on overseas threats, and enable the Command decision makers to implement measures to keep deployed AMC, AFRC, and ANG forces safe. Also, CONUS threats must now be addressed due to Homeland Security Task Force and ongoing Operation Noble Eagle. For example, Information Warfare and FP risk assessments must include all threats during all stages of the mission planning and execution process.

4.6.4.2. TWG all-source threat analysis and FP recommendations are forwarded to the AMC/DO. The DO established policy is based on these recommendations and is quickly disseminated and available via the AMC/IN SIPRNET homepage (**http://www.amcin.scott.af.smil.mil**) on Intelink-S (classified Internet), secure voice/fax, or by other means. The TWG also disseminates its products to commercial carriers flying DoD missions.

4.6.4.3. The TWG makes FP recommendations on individual missions by objective analysis of potential threats and careful consideration of mitigating FP measures. Key TWG tools used in this process include:

4.6.4.3.1. Secure Launch Country List and Monitor Country List. Unclassified document which identify countries where the security situation is fluid and could deteriorate with little warning, creating such dangerous conditions that AMC aircraft scheduled to fly there would be at serious risk. A country is added to the Secure Launch list if it meets at least one of these criteria: SIGNIFICANT or HIGH terrorism threat as assessed by DIA and/or the AOR; has demonstrated chronic instability in an area of AMC operations; or contains a large US military presence or AMC footprint that may provide an alluring target for anti-US elements. A Monitor country is one that has potential to become a high-risk environment, but does not meet Secure Launch criteria.

4.6.4.3.2. Phoenix Raven Required Locations List. An unclassified document that identifies airfields where security is unknown or unacceptable, and where additional threats, or the level of threat, indicate a need for specially trained security forces to provide dedicated aircraft security.

4.6.4.3.3. Man Portable Air Defense (MANPAD) Vulnerability Risk Assessment. A classified document that evaluates the portable SAM threat.

4.6.4.3.4. Operational Risk Management Matrix. A classified document that evaluates overall criminal, terrorist, military, information warfare, and medical threats and FP mitigating measures. It forms the primary baseline to determine the acceptability of individual airfields.

4.6.4.3.5. Risk Assessment. A classified document. Published analysis that details threats and FP recommendations at Secure Launch locations where AMC operates. The TWG currently maintains 170+ Risk Assessments covering 82 countries. These are maintained in the AMC Virtual Risk Assessment Database (VRAD). The VRAD can be searched by airfield, ICAO number, or country, and also provides countrywide recommendations.

4.6.4.3.6. AMC Policy Matrix. A classified comprehensive summary of all AMC/DO policy. Exceptions to this policy must be requested and approved by the AMC/DP (or the TACC/CC if mission is in execution.) Used for planning and executing AMC missions.

4.6.4.3.7. Virtual Threat Assessor. The AMC Virtual Threat Assessor (VTA) uses web-based technologies to leverage multiple national level databases, providing a concise summary of threat data on nearly all airfields worldwide. The VTA also provides links to other analysis products such as imagery, National Imagery and Mapping Agency (NIMA) Advanced Airfield Information (AAFIF), theater assessments, mission reports, DIA and OSI reports, and open source information.

4.7. Unit Level Force Protection (FP). Operations Support Squadrons (OSSs) are primarily responsible for providing intelligence to support FP for in-garrison, in-transit, and deployed units. This includes providing your local TWG, FPWGs, Battlestaff, and aircrews with intelligence support and terrorist threat advisories, as needed. This support is accomplished by providing current, all-source intelligence products, analysis, and briefings on terrorist capabilities, tactics, deployment/employment and ongoing threat situation.

4.7.1. SIO Responsibilities. SIOs will designate, in writing, an intelligence officer or NCO to provide support to FP. The designated individual must have access to SCI and HUMINT Control System (HCS) information. The selected individual needs to receive appropriate training and can coordinate training requirements through HQ AMC/INXT, Formal Training.

4.7.2. FP Intelligence Designate Responsibilities. Individuals designated to provide intelligence support to FP need to develop and maintain a continuity book outlining intelligence FP responsibilities as well as checklists identifying key tasks performed in researching, accumulating, preparing and presenting FP intelligence and formalizing the processes. These activities should include analyzing incoming intelligence for FP value and impact on the unit's mission, current and planned operations, exercises, air shows, significant Morale, Welfare, and Recreation (MWR) events, and rapidly disseminate significant intelligence to the wing TWG, Battlestaff, FPWGs, Security Forces, and key individuals of subordinate and lateral units, higher headquarters, other agencies and services, as needed. A debriefing checklist should also be developed that includes Essential Elements of Information (EEIs). Any terrorist-related information obtained during debriefs should be reported through warning reports, FP summaries, briefings, liaison, or other appropriate means. In addition, a FP database should be developed for documenting any lessons learned from FP events. Other responsibilities should include the following:

4.7.2.1. Be actively involved with the local TWG in developing realistic terrorist training scenarios for use during installation exercises.

4.7.2.2. Participate in installation vulnerability assessments IAW AFI 10-245, *Air Force Antiterrorism Standards*.

4.7.2.3. Be an active member and participant in the installation-level TWG IAW AFI 10-245.

4.7.2.4. Support local OSI in the development of the installation threat assessment.

4.7.2.5. Coordinate with local OSI to ensure all available FP information is incorporated into intelligence support to FP (external and internal training, operational support, and support to commanders).

4.7.2.6. Pre-deployment/deployment procedures. Establish intelligence procedures and checklists for intelligence FP support and activities for pre-deployment and deployment phases. These procedures should include intelligence roles and responsibilities in pre-deployment and deployment briefings for wing members, aircrew, and commanders. Additionally, procedures/checklists should include methods of coordination with appropriate NAF, theater, and deployed base TWGs to ensure all FP information is available to deploying personnel prior to departure.

4.7.2.7. Employment/sustainment procedures. Establish intelligence procedures and checklists for intelligence FP support during the employment and sustainment phases of operations. These procedures should include: establishing the Threat Working Group meeting schedule, ensuring SIPRNET/JWICS connectivity, coordinating with local intelligence agencies (including U.S. Embassy personnel, host nation security, and other U.S. Service organizations), checking with the local OSI for reporting and information, ensure appropriate message traffic system is set up to include FP information, and how to provide intelligence updates on local (deployed location) anti-terrorism restrictions and security measures.

4.7.2.8. Re-deployment procedures. Establish intelligence procedures and checklists for intelligence FP support during the re-deployment phase of operations. These procedures/checklists should include how to provide FP support to all personnel at the deployed location throughout the re-deployment phase, even as numbers of personnel dwindle. Additionally, procedures/checklists should include a way to capture and transmit deployment-specific lessons learned.

4.7.2.9. Even though these tasks are accomplished by the FP appointee, the responsibility for accomplishing these tasks ultimately falls on the SIO.

4.7.3. Lessons Learned. All lessons learned need to be documented and forwarded to the wings' TWG, FPWG, and MAJCOM for any required actions. Ensure these lessons learned are documented in an appropriate database.

4.7.4. Intelligence FP Training Program. The intelligence Force Protection Designate should establish an internal FP intelligence training program. This program should include an OI detailing how the FP intelligence training program will be conducted. Qualifications for intelligence personnel should be established to certify trainer prior to conducting FP training. The FP training program should prepare all assigned intelligence personnel to perform FP responsibilities. This training should be included as part of the units Initial Qualification Training and continuous internal training and should be documented in the individualss training record. Local training programs should include the following:

- Understanding terrorist Tactics, Techniques, and Procedures (TTPs)
- Conducting FP focused predictive analysis
- Terrorist threat methodologies
- FP Threat Conditions and terrorism threat levels
- Current terrorist threat

- In-place FP procedures, reporting directives, and communications means
- Country restrictions such as travel, lodging, dining for countries in AOR or where TDYis likely for assigned personnel
- Development of tailored threat assessments and assessing terrorist threat levels
- Supporting FP planning
- Supporting vulnerability assessments
- Locating sources of FP intelligence
- FP legal considerations (Intelligence Oversight policy)
- Location and content of read files

4.7.5. FP External Training Program. In conjunction with local OSI and SF personnel, an external FP intelligence-awareness program for designated SF personnel should be developed. Much of this information should also be made available to aircrew members as required by real-world deployments and operations. This training should be developed similar to Aircrew Intelligence Training and should provide information on the following:

- Understanding terrorist TTPs, operational capabilities, intentions, tactics and courses-of-action
- Current terrorist threat
- Terrorist threat levels
- Locating sources of FP intelligence
- Country restrictions such as travel, lodging, dining
- MANPAD threats, tactics, and mitigation measures
- Location and content of read files

4.7.6. AOR-specific FP training resources. These links may be used to get the AOR intelligence update for overseas TDY/PCS/Leave. Classified sites listed on this page must be accessed via SIPRNET.

US Central Command (USCENTCOM)

Classified: Ccj2_intel-s.centcom.smil.mil/jic/terrorism/summary/indextmp.htm

Unclassified: **http://www.centcom.mil**

US Southern Command (USSOUTHCOM)

Classified: **164.232.22.173**

US European Command (USEUCOM)

Classified: **http://www.eucom.smil.mil.ecsm**

Unclassified: **http://www.eucom.mil/hq/ecsm**

US Joint Forces Command (USJFCOM)

Classified: **157.224.120.150/index.htm**

US Pacific Command (USPACOM)

Classified: **http://www.hq.pacom.smil.mil**

Unclassified: **http://www.pacom.mil/homepage.htm**

4.7.7. As the Global War on Terrorism progresses, FP is becoming one of intelligence's primary functions. Establishing a solid FP program will provide your leadership with needed information to make sound informative FP decisions. FP should be considered in all stages of operations. All intelligence personnel, regardless of position or title, should do basic FP analysis as part of daily intelligence operations. FP should not be viewed as an additional duty. Additional information on FP may be found on the HQ ACC Intelligence homepage located at **https://in.acc.af.mil/sttp/WingSdqnFunctions/WingandSqdnIndex.htm**.

Chapter 5

BRIEFINGS

5.1. General. This chapter covers basic intelligence briefings required at the unit-level and some recommended techniques for developing and presenting them properly. By definition, a briefing is a brief presentation offering critical information necessary to accomplish a specific purpose. The "ABC" rule of thumb is always applicable (**A**ccuracy, **B**revity, and **C**larity). Purpose is what drives the content and scope of any briefing. When completed, the audience should clearly understand the information presented and the impact that information poses to current and future operations. To prepare a well-focused, pertinent briefing requires an understanding of enemy capabilities, tactics, and equipment, as well as the specific needs of the audience.

5.2. Security Considerations. Most intelligence briefings are developed from classified information. The classification of the information extracted and used generally determines the classification of the briefing. Equipment used in developing and presenting classified briefings must be properly accredited and marked. Responsibility for ensuring the security of the information presented rests solely on the briefer. The briefer must ensure that visual aids, handouts, and notes are properly marked in accordance with DoD 5200.1-PH, DoD, *Guide to Marking Classified Documents*, and safeguarded in accordance with DoD 5200.1R, *Information Security Program*. Classified and/or sensitive information must only be presented in a properly secured area and only to personnel with the appropriate security clearance and a verified "need-to-know." Sensitive Compartmented Information (SCI) requires even more stringent security measures. You should consult your servicing Special Security Officer (SSO) for additional requirements for SCI briefings.

5.3. Briefing Development.

5.3.1. The first step in briefing development is to identify the specific need and purpose of the briefing. The next issue to consider is the background of the audience and its level of prior knowledge on the subject being briefed. Available methods (overhead projector, computer projector, no projection equipment, etc.) of presentation play a key role in determining the presentation medium (overhead slides, Power-Point presentation, wall charts, etc.) Regardless of the presentation method used, the key is that it's the best possible method available, under the circumstances. It's always a good idea to maintain blank, pre-formatted, overhead slides that can be quickly penned in and displayed, just in case all else fails. These are also great time savers during time crunches.

5.3.2. If the briefing refers to a location or incident, use a map or chart to graphically depict that information. If the briefing discusses an installation, try to get imagery so the information can be connected to a mental picture. Keep in mind that a picture can be worth a thousand words when properly and accurately used, whether the "picture" is a plotted chart, photograph, or a statistical graph. On the flip-side, "eye-candy" with no clear connection to the information being presented usually detracts from the effectiveness of the briefing.

5.3.3. With constant focus on the purpose of the briefing, research and analysis must be accomplished. During research, all available sources are scoured to gather pertinent, readily available information. Analysis clarifies the impact of the information gathered and identifies any gaps that may require further research. When necessary, external research reaches out to higher-headquarters and other organizations for additional information and assistance. Searching Intelink/Intelink-S or issuing

a RFI are only a couple of options available to unit-level intelligence for external research. See chapter IV for a more thorough discussion on analysis.

5.3.4. The best time to refine a briefing is while it's being developed. Play "devil's advocate" as the briefing is being built. The wide variety of potential audiences and purposes makes a definitive list of briefing dos and don'ts impossible, but a few things to keep in mind include:

- By definition, a briefing is short, concise and direct. Present all necessary and pertinent information, but strive to keep briefings as short as possible.
- Remain organized and focused on the purpose.
- Strive to be the "Subject Matter" expert on the material to be briefed.
- Use neat and clear visual aids that make a genuine contribution to clarity.
- Know the audience, situation, and any special requirements.
- Anticipate questions, research and be prepared to discuss answers, have "hip pocket data".
- If at all possible, be familiar with and prepare briefing facilities in advance.
- Above all-be honest! If you don't know the answer to a question, say so. Then go find the answer and provide it as soon as possible afterward.

5.4. Types of Briefings. This section addresses the most common briefings required within AMC. Following the discussion are sample checklists for use in preparing/presenting each primary type of briefing. Neither the discussion nor the checklists are all-inclusive of briefing formats or data requirements. They are examples and should be further tailored to your unit's particular requirements.

5.4.1. Current Intelligence Briefing (CIB).

5.4.1.1. The CIB is typically an in-garrison briefing and part of the unit's current intelligence program. There is no standard format for a CIB. These briefings are as varied as the list of potential topics, audiences, and briefers. However, the example checklist provided on page 39 and this discussion may help generate ideas for establishing your unit's current intelligence program. Additionally, consult your commander/audience to ensure their needs are met and their preference for format is followed.

5.4.1.2. A good current intelligence program is a critical element of in-garrison support. If it is directed properly, it will ensure a wide knowledge base on current worldwide political and military affairs. A good program will greatly decrease the spin-up time required when a crisis kicks off. Finally, the current intelligence support you provide to your unit while in-garrison can play a large role in establishing your credibility as an intelligence professional.

5.4.1.3. Three major aspects to consider when developing a current intelligence program include currency, relevancy, and special requirements. First of all, topics presented at a CIB must be current developments. Secondly, they must be relevant to the unit's mission and planned or probable operating areas. Lastly, CIB topics should take into consideration any special equipment requirements, unique unit capabilities or limitations, and the impact the topic has on those requirements. Always pay special emphasis to threats that directly affect the way your unit will operate.

5.4.1.4. CIBs often generate questions from the audience that require research and follow-up. Obtaining answers to these inquiries must receive the highest priority, as the information is impor-

tant and your credibility is at stake. To preserve continuity in your briefing program, maintain a record of current intelligence briefings, questions, and responses.

5.4.2. Crisis Action Team/Battle Staff Briefing.

5.4.2.1. The Crisis Action Team (CAT) or Battle Staff (BS) generally meets at regular intervals during crises and contingencies. These meetings bring together the unit's senior leaders, and technical experts. The purpose is to review the current situation and assess the sufficiency of the unit's intended courses of action. Your role in the process is to provide the CAT/BS with the adversary's current status and potential/probable courses of action, or COAs. The unit's COA is strongly dependent upon the information you provide. Additional, ad hoc briefings and updates may be required as the situation changes. Be thorough but brief, as the members of the CAT/BS are extremely busy. Focus on relevant information that may have impact on mission accomplishment.

5.4.2.2. If at all possible, remain for the duration of each CAT/BS session. It's important to understand how each representative of the meeting contributes to the effort at hand, and how the information you present impacts them. You'll also be cognizant of schedule changes, base threat updates, weather, support, maintenance or engineering changes that may impact your ability to operate.

5.4.3. Pre-Deployment Briefing.

5.4.3.1. Intelligence personnel should brief all deploying unit members, especially those deploying to contingency theaters. Unit members deserve to know what threats they may face in the forward location, and to hear about these threats in a face-to-face fashion so they can ask questions. At the conclusion of the briefing, the audience should understand the military/political situation that generated the deployment. They should know the desired end-state the theater commander intends to achieve. They also need to know the general capabilities of enemy systems posing a threat to the deployment location, as well as other threats, such as medical hazards, criminal and terrorist threats, likely reaction of local populace to the unit's presence, etc. Obviously, intelligence will have to work with other functionals, such as OSI, SF, medical personnel, as well as in theater intelligence personnel. As time permits, take the opportunity to brief support personnel on updates to the military and political situation. This provides an understanding on why they are deployed, keeps them in the loop on what is happening, encourages camaraderie and motivates them.

5.4.3.2. Aircrews should be briefed separately from ground personnel. In addition to the pre-deployment items briefed to ground personnel, aircrews need to be briefed on specific en route and in-theater weapon systems that they may encounter. If the deployment timeline permits, prepare and present in-depth theater study briefings that include capabilities and limitations of enemy threat systems, firing doctrine, recognition features, force employment doctrine, etc. Theater Special Instructions (SPINS) covering E&R information should also be discussed at length as well as individual ISOPREP reviews. Check to see if training aids have already been developed for the operation you will participate in (i.e., country weapon system guides, vegetation guides, etc.) A lot of this information can normally be found in theater "In-Chop" briefings that are usually briefed when first entering the AOR.

5.4.4. Pre-Mission Briefing.

5.4.4.1. All aircrews should receive a pre-mission briefing prior to taking off for employment sorties. These briefings should be conducted in concert with weather, mission planners, and the tac-

tics officer. The end result should ensure the crew knows where they're going, what they're going to do, all potential threats along the route, and tactics to be used to defeat or mitigate those threats.

5.4.4.2. The mission route should always be plotted as an overlay on a suitable situation display. All OB data with direct or potential impact on the mission must be displayed along with applicable detection/tracking/engagement envelopes. Begin the briefing by securing the room, announcing classification and "current as of" time of the briefing. Briefly discuss significant political/military developments, the general battle situation, and current disposition of friendly (to include AWACS/ Tanker orbits, etc) and hostile forces as they affect the mission. Remind crewmembers to review ISOPREPs. Clearly point out latest known positions and status of downed aircrew.

5.4.4.3. The most intensive part of the briefing should focus on the mission route. This portion begins with discussing actual/potential threats from the time that the crew departs the briefing room until they return for debriefing. When briefing route threats, "fly the mission route" with the crew. Follow way-point by way-point along the route and discuss each known and potential threat along the way, including when/where the threat can detect and engage the mission aircraft. Provide pertinent information concerning conditions and threats in the objective/target area. When briefing the return route, don't forget to factor in potential enemy movements that could further impact the mission.

5.4.4.4. Step Brief. The Step Brief is actually an extension, and an integral part, of the pre-mission briefing. After the crew leaves your briefing area, they have several other stops to make prior to "stepping" to the aircraft. The time-lapse between your briefing and their take-off can vary widely depending on the unit, crew, mission, and situation. You must stay attuned to scheduled takeoff times and slips. If significant new information is received that could impact the crew's mission, you need to get that information to them. The theater may issue Pilot Update Codes (PUCs) or Intelligence Update Codes (IUCs) when new information or threat locations become available. These PUCs/IUCs may be posted within the operations area so aircrew members can be advised whether they need to get additional information before they step. You need to have a process in place to ensure that such information gets to the crew before they take off. This may entail a crewmember dropping back by Intel on his/her way out the door. It may require Intel to have someone waiting at the doorway to the crew bus. Under some circumstances, the information may be significant enough to warrant sending an Intel troop to the aircraft to brief, or even recalling the crew for an in depth update. Flexibility, integrity, and common sense must guide the development of such procedures.

5.4.5. Shift Changeover Briefing.

5.4.5.1. This is the final responsibility for each shift. Its purpose is to recap all major events occurring since your counterpart was last on duty. You want to ensure the oncoming shift is not caught uninformed or unprepared on any significant items. Before beginning the shift changeover briefing, your relief should review the significant events log/board, incoming/outgoing message logs, current OB and situation displays, etc.

5.4.5.2. During your shift changeover briefing, review status boards, message traffic, the ATO, and shift log with the on-coming crew. Cover equipment status, personnel status, and any changes in procedures since last shift. Summarize events in the political/military (POL/MIL) situation, local area threats, missions tasked, and missions still out that will need to be debriefed. Discuss significant changes (or lack of change) in enemy and friendly force disposition. Allow at least 30

minutes to deliver the briefing and answer questions, more if needed. When you walk out the door, the new crew should know, in a nutshell, everything significant that occurred since they last walked out the door.

5.5. Briefing Checklists. The importance of instructions and checklists cannot be overemphasized. Instructions provide comprehensive direction and guidance for accomplishing major/critical tasks. Checklists are abbreviated instructions that list significant tasks and serve as a memory jogger and accounting tool. The following figures provide samples that may be tailored for use as unit briefing checklists.

INTELLIGENCE CHECKLIST		PAGE 1 OF 1 PAGES		
TITLE/SUBJECT/ACTIVITY **CURRENT INTELLIGENCE BRIEFING**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
Note: *It should be readily apparent why you are covering this topic. If it is not apparent, then you must explain the reasoning. Always ask (and answer) "Why am I briefing this to my commander and crews?" If you can't properly answer this question, then reevaluate the need for the topic.*				
1.	Secure the room (radios/bricks/telephones off, doors/windows closed, guards posted, clearances verified).			
2.	Security classification.			
3.	Information "Current as of" time.			
	Note: *Each topic you discuss should follow steps 4 - 6 below.*			
4.	A brief background on the topic (if appropriate).			
5.	Discuss main points of topic (only the ones that impact mission/mission readiness).			
6.	Impact/significance to your unit.			
7.	Solicit questions.			
8.	Security classification and "Current as of" time reminder.			
9.	Log briefing in events log.			

INTELLIGENCE CHECKLIST		PAGE 1 OF 1 PAGES		
TITLE/SUBJECT/ACTIVITY **CAT/BS BRIEFING**		OPR	DATE	
NO.	ITEM	YES	NO	N/A
1.	Secure the room (radios/bricks/telephones off, doors/windows closed, guards posted, clearances verified).			
2.	Security classification.			
3.	Information “Current as of” time.			
4.	Significant political/military developments affecting unit (use displays).			
5.	Threat to home station/local area situation (terrorist, sabotage, NBC, etc.).			
6.	Indications of impending attack (home station and bases unit aircraft may operate).			
7.	Deployment route threats (if applicable).			
8.	FOB security situation (threat condition/security level/ terrorist and criminal threat).			
9.	Friendly force disposition/situation (if applicable).			
10.	Enemy force disposition/OB.			
11.	Areas of major engagements (FLOT/FEBA, etc.).			
12.	CSAR events and downed airmen.			
13.	Enemy intentions estimate/Probable course of action.			
14.	OPSEC/COMSEC reminder.			
15.	Solicit questions.			
	Security classification and “Current as of” time reminder.			
	Log briefing in events log.			

INTELLIGENCE CHECKLIST		PAGE 1 OF 1 PAGES		
TITLE/SUBJECT/ACTIVITY **PAX PRE-DEPLOYMENT BRIEFING**		OPR	DATE	
NO.	ITEM	YES	NO	N/A
1. Secure the room (radios/bricks/telephones off, doors/windows closed, guards posted, clearances verified).				
2. Security classification.				
3. Information "Current as of" time.				
4. Summary of significant military/political situation and events causing deployment (use displays). Review EXORD/DEPORD tasking. Answer the question, "Why are we deploying?"				
5. General description of the deployment location: (Focus on how each may/will affect the deployment location, deploying forces, and operations)				
a. Regional and country background (political, military, cultural, economic, and geographic)				
b. Anticipated reaction of local populace to deploying forces				
6. General status of forces in the deployment theater (use displays):				
a. Disposition of US and other friendly forces				
b. Disposition of hostile forces				
7. Threats to the deployed location (focus on actual and probable threats)				
a. Conventional (munitions and delivery systems)				
b. NBC (munitions and delivery systems)				
c. Other threats, including civil unrest, terrorist activity, medical, and environmental (Developed in concert with the Threat Working Group).				
8. OPSEC/COMSEC reminder.				

9. Solicit questions. 10. Security classification and “Current as of” time reminder. 11. Log briefing in events log.			

INTELLLIGENCE CHECKLIST		PAGE 1 OF 2 PAGES		
TITLE/SUBJECT/ACTIVITY **AIRCREW PRE-DEPLOYMENT BRIEFING**		OPR	DATE	
NO.	ITEM	YES	NO	N/A
1. Secure the room (radios/bricks/telephones off, doors/windows closed, guards posted, clearances verified).				
2. Security classification.				
3. Information "Current as of" time.				
4. Summary of significant military/political situation and events causing deployment (use displays). Answer the question, "Why are we deploying?"				
5. General description of the deployment location: (Focus on how each may/will affect the deployment location, deploying forces, and operations)				
a. Regional and country background (political, military, cultural, economic, and geographic)				
b. Anticipated reaction of local populace to deploying forces				
6. General status of forces in the deployment theater (use OB and Situation displays):				
a. Disposition of US and other friendly forces				
b. Disposition of hostile forces				
7. Threats to the deployed location and alternate/divert/abort airfields (focus on actual and probable threats)				
a. Conventional (munitions and delivery systems)				
b. NBC (munitions and delivery systems)				
c. Other threats, including unconventional forces, civil unrest, terrorist activity, medical and environmental hazards (developed in concert with the Threat Working Group).				

8. Areas of major engagement (if any). 9. Potential/anticipated enemy reaction to the deployment. 10. Potential en route flight hazards (Spectrum Interference Resolution (SIR), naval, SAM, AAA, aircraft. 11. Theater Evasion and Recovery requirements and procedures. a. Hostile, friendly, and neutral areas. b. Evasion geography, Selected Area For Evasion (SAFE) /SAFE Area Intelligence Description (SAID).			

INTELLIGENCE CHECKLIST		PAGE 2 OF 2 PAGES		
TITLE/SUBJECT/ACTIVITY **AIRCREW PRE-DEPLOYMENT BRIEFING (Continued)**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
	c. Recommended evasion actions (if applicable). d. Theater recovery and authentication procedures (call sign/frequencies of SAR Forces--word, letter, and number of the day). e. Evasion Plans of Action f. Requirements to sanitize uniforms prior to at-risk missions. g. ISOPREP Review h. Specific instructions contained in OPLAN, ACO, SPINS, etc. i. Review of Evasion and Recovery (E&R)/Personnel Recovery (PR) Kits 12. Review Essential Elements of Information (EEIs) the crew may be in a position to observe (refer to AMCI 14-102, OPLAN, CONPLAN, etc). 13. Debriefing and reporting requirements and instructions to include debriefing location and POC. In-Flight Report (INFLTREP) Mission Report (MISREP) Spectrum Interference Resolution (SIR) Reporting 14. OPSEC/COMSEC reminder. 15. Solicit questions. 16. Security classification and “Current as of” reminder.			

17. Log brief in events log.			

INTELLLIGENCE CHECKLIST		PAGE 1 OF 2 PAGES		
TITLE/SUBJECT/ACTIVITY **PRE-MISSION BRIEFING**		OPR	DATE	
NO.	ITEM	YES	NO	N/A
1. Secure the room (radios/bricks/telephones off, doors/windows closed, guards posted, clearances verified). 2. Emergency exit/regroup procedures. 3. Security classification. 4. Information "Current as of" time. 5. Brief review of general battle situation (keep it brief and to the point and use displays.) a. Significant geo-political developments with impact on operations. b. Significant changes in ground force disposition/OB (includes unconventional, guerrilla, and terrorist forces.) c. Significant changes in naval force disposition/OB. d. Significant changes in air force disposition/OB. e. Significant air activity, friendly and hostile, with potential impact on mission. f. Current and 12-hour projection of FLOT, FEBA, and FSCL trace. 6. Mission Objective/s (display graphically in appropriate scale to show relationship to rest of situation, include imagery of objective area when appropriate.) 7. Mission threat assessment (point by point route threat assessment beginning at doorway from briefing room and concluding at doorway to debriefing location.) a. Immediate area threats – From briefing room to takeoff. b. Ingress route threats – Show detection, tracking, and engagement envelopes for all pertinent threats.				

(1) Surface to air defenses (SAM, AAA, includes naval.) (2) Airborne defenses (CAP points, alert forces, etc.) (3) Electronic threats (spectrum interference/ECM, EW/GCI, passive detection systems.) c. Objective area threats – includes same considerations as for 7.b. d. Egress route threats – includes same considerations as for 7.b. e. Anticipated threats at recovery, divert, abort fields (include imagery of these fields.)			

INTELLLIGENCE CHECKLIST		PAGE 2 OF 2 PAGES		
TITLE/SUBJECT/ACTIVITY **PRE-MISSION BRIEFING**		OPR	DATE	
NO.	ITEM	YES	NO	N/A
8. Evasion and Recovery information (in concert with SERE Specialist, when available.) a. Review SAR data on known survivors believed in the area of mission, include last known location, call sign, contact time, and SAR codes the day of loss. b. Review SAFEs/SAIDs/Designated Areas for Recovery (DARs) applicable to mission (location and description.) c. Theater authentication and recovery procedures (include word, letter, and number of the day, and SARNEG). d. Reminder to sanitize uniforms. e. Distribute E&R/PR kits (Crew members must sign for them.) f. Create/Review/Update EPA – Assist/provide recommendations based upon mission and overall situation. g. Reminder to review and annotate ISOPREPs 9. Debriefing and Reporting Instructions: a. Review EEIs crew may be in a position to observe. b. Review in-flight reporting requirements/procedures. c. Specify debriefing location, POC, and contingency plans. d. Remind of MISREP and Spectrum Interference Resolution (SIR) reporting requirements. 10. OPSEC/COMSEC reminder. 11. Solicit questions.				

12. Review Step-Update Briefing procedures to include PUCs/IUCs. 13. Restate classification and current as of time. 14. Log briefing in events log. 15. Fill in header information on debriefing form to prepare for debriefing.			

INTELLIGENCE CHECKLIST		PAGE 1 OF 1 PAGES		
TITLE/SUBJECT/ACTIVITY **SHIFT CHANGEOVER BRIEFING**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
Note: *Have your relief review the significant events log/board, message traffic (both incoming and outgoing), OB/Situation Displays, and ATO prior to briefing.*				
1.	Secure the room (radios/bricks/telephones off, doors/windows closed, guards posted, clearances verified).			
2.	Information "Current as of" time.			
3.	WATCHCON/DEFCON level.			
4.	Significant military/political events.			
5.	General disposition of enemy forces to include air, ground, and naval.			
6.	Areas of major engagement (FEBA/FLOT/FSCL).			
7.	Probable courses of enemy action.			
8.	Local area situation to include FPCON, MOPP level, enemy actions, and Terrorist/Sabotage/Subversion actions.			
9.	Open Search And Rescue (SAR) cases (survivor's last known position, condition, and call sign.)			
10.	Missions in progress and estimated debrief times.			
11.	Applicable information from theater MISREPs; any PUCs/IUCs updates.			
12.	Next Pre-mission/CAT/BS/WOC/Commander's Update briefing.			
13.	Any major problems encountered during the last shift, and any suggested or implemented solutions.			
14.	Systems/supply status.			
15.	Any actions that require follow up by next shift.			

16. Changes in policy/procedures to make the shop more efficient.			
17. Ensure the shop is in good order, classified accounted for, and the IN events/message log is up to date.			
18. Log shift change in events log.			

Chapter 6

REPORTS

6.1. General. The primary purpose for unit-level reporting is to provide information up-channel concerning unit status and mission results. Unit reporting is tactical and generally perishable in nature. This perishable data is time-sensitive and useless if not delivered in a timely fashion and useable format. Reporting is a critical element of intelligence operations. It is the product your intelligence element provides to HHQ to enable leadership at all levels to develop the most comprehensive picture of the situation possible. Well-written, timely intelligence reports can increase future mission effectiveness and save the lives of your crews, fellow unit members, and other friendly forces.

6.2. Reporting Requirements.

6.2.1. During normal, day-to-day, peacetime operations, AMCI 14-102, *Intelligence Debriefing and Reporting*, defines intelligence reporting responsibilities for units under the Operational Control (OPCON) of AMC. This instruction provides detailed direction on primary and alternate reporting formats, procedures, and media. Every member of your intelligence team must be intimately familiar with this instruction, the prescribed formats, and channels of reporting. Units must develop specific local operating instructions and checklists to aid their members in understanding and accomplishing reporting processes.

6.2.2. While deployed to an operational theater, you will normally Change OPCON (CHOP) to theater command authorities. Units CHOP'd to the theater must be prepared to accomplish reporting as directed by the theater. You can find reporting instructions ahead of time by reviewing the Intelligence Annex to OPLANS or Concept Plans (CONPLANS), theater-reporting instructions, TTPs, SPINS and also by reviewing theater Intelink-S web sites. If confusion or problems are encountered, request clarification from the theater intelligence staff. The keys to an effective reporting program are to understand requirements, formats, primary and alternate means of transmission, and to develop processes and conduct regular training tailored to meet these requirements.

6.3. Report Content. This is the most important aspect of intelligence reporting. Messages must be accurate, well written, concise, and contain all relevant information. Strong in-garrison training will pay dividends of efficiency and accuracy during contingency or combat operations. Develop and use detailed checklists for report generation to ensure all required information is addressed. A transmitted report should answer what, where, when, how, why, what it means, and what's next. Check for simple errors like coordinate plotting/extraction, time zone errors, references to place names without associated coordinates, and use of acronyms or jargon that may not be understood outside of your unit. Develop and implement quality control processes that are commensurate with the criticality and time sensitivity of the data being reported. Developing a complete, accurate word picture that conveys the most amount of information in the least amount of time is the ultimate goal of any military reporting program.

6.4. Report Timeliness. The process of prioritization must be constantly applied to reporting. Perishable information on a new threat or tactic may need to be submitted immediately, even if it delays other normal reporting requirements. Personnel submitting unit reports must have the experience and training to make such calls. Be prepared to use alternate methods of transmission. Interruptions in primary transmission

may require rapid, flexible, and even creative work arounds. Once again, in-garrison planning, process development, and training offer the greatest chance of success under the worst conditions.

6.5. Report Formats.

6.5.1. The most challenging aspect of writing and submitting reports lies in report formats. Today, several different formats and reporting systems are fielded. You may encounter situations when different elements within the same theater demand different reporting formats or levy different criteria on the same data. The best way to minimize the impact of such situations is to conduct comprehensive in-garrison preparation whenever possible.

6.5.2. United States Message Text Format (USMTF). USMTF is the closest we've come to having a DoD-wide, standardized reporting format. With exposure, training, and guidance, extracting data from messages produced in USMTF can be much quicker for the user. The bottom-line, unless directed otherwise by the command authority to whom you're CHOP'd, USMTF is assumed to be the required format for military reporting.

6.5.2.1. The Defense Information Systems Agency (DISA) is responsible for maintaining DoD information technology standards and conventions. The Center for Standards, part of the Joint Information Engineering Organization, is the DISA-designated configuration manager for the USMTF Program. To assist in DoD-wide implementation of USMTF, DISA has developed a comprehensive CD-ROM titled 'USMTF USER FORMATS'. This CD provides standards, training, and message generation applications. To obtain a copy of this product, contact the AMC Command Dissemination Manager or visit **http://www-usmtf.itsi.disa.mil/**.

6.5.3. On-Line Forms. AMC/IN provides on-line forms for intelligence reporting requirements directed by AMCI 14-102, *Intelligence Debriefing and Reporting*. The forms can be found on the AMC/IN Intelink-S web page at **http://www.amcin.scott.af.smil.mil**. On-line reporting is the preferred method unless SIPRNET connectivity is unavailable or theater authorities direct otherwise. Several commands and agencies are also developing the means to satisfy reporting requirements via on-line, fill-in the blank forms.

6.6. Types of Reports.

6.6.1. In-Flight Report (INFLTREP). The INFLTREP is used by pilots and aircrews to report mission results or any other tactical information sighted of such importance and urgency that the delay, if reported by normal debriefing, would negate the usefulness of the information. This message is transmitted by voice only. Aircrews report INFLTREPs to the nearest friendly command post, Air Mobility Element (AME), Wing Operation Center (WOC), or Tanker Airlift Control Element (TALCE). The receiving entity should immediately forward INFLTREP data to unit intelligence. If necessary, intelligence personnel will generate an initial Intelligence Report (INTREP) based upon the INFLTREP information. This INTREP will be transmitted at immediate or higher precedence. After a thorough debriefing, a follow-up MISREP will be transmitted incorporating the initial INTREP and providing all additional pertinent data. There is no set format for an INFLTREP, therefore, unit intelligence should coordinate with their local Command Post (CP), WOC, and operational squadrons to develop an agreed upon format. Examples of the INTREP and MISREP are available in AFI 14-102, Debriefing and Reporting, Attachments 2 and 3. Unless directed otherwise, use the AMC On-Line MISREP form.

6.6.2. Mission Report (MISREP). The MISREP is used by intelligence personnel to convey pertinent information that relates to aircraft and mission execution. Reports can range from a few lines to several pages depending on the mission and information observed. MISREPs are sent at immediate or higher precedence as outlined in AMCI 14-102, *Intelligence Debriefing and Reporting*. Because time limit is short, units must be familiar with theater reporting requirements and prepare in advance to transmit these reports. Although various MISREP report shells exist, ensure unit debriefing checklists mirror the applicable MISREP format and includes all fields required in the MISREP. Information contained in the AMC/IN MISREP report consists of the following:

6.6.2.1. General Information. The general information section requires specific overall report data, including the classification of the report and all pertinent handling caveats. The "TO;" e-mail address is defaulted to an AMC/IN developed address list, but other addresses may be added. The "FROM:" block should contain the name and rank of the person filing the report. Be sure to fill in a valid, current, email address in the "E-MAIL ADDRESS:" block to allow return feedback or questions if they arise. The rest of the information required is fairly self-explanatory and concerns the report number, mission number, etc.

6.6.2.2. Mission Information. The next general section of the online MISREP requests specific information collected during the mission. This includes information on each airfield the mission visited, weather data, SAM encounters or indications received, AAA encounters, and information describing attempts to intercept the mission aircraft. FP information is solicited in a free-text remarks block. An additional remarks block is available to report any other information of value not specifically addressed elsewhere in the report. All of the information requested by the online MISREP form is important to subsequent mission planning, threat analysis, and trend analysis, so make every effort to obtain and report all pertinent data. Issues to consider in these areas include:

6.6.2.2.1. Weather Data. Weather is a factor that can drastically affect the success of air operations. Consequently, MISREPs should include detailed weather data encountered and the effects it had on the mission.

6.6.2.2.2. SAM Data. SAMs present a critical threat that can be difficult for any aircraft to counter, especially large, relatively slow moving AMC aircraft with limited maneuverability. The employment of SAMs not only directly threatens the mission aircraft, but the act also speaks volumes on the capability and intent of the adversary. It's absolutely critical to glean all possible information on such occurrences, but you must also keep in mind that SAM reporting can be difficult for aircrews. While some SAM sites are readily identifiable, many are mobile, fired from self-propelled vehicles, or shoulder-fired, making it difficult to locate the sites. Be knowledgeable of these limitations, but gather all information possible.

6.6.2.2.3. Anti-aircraft Artillery. AAA is often used for close-in, point defense of areas/facilities of military importance. In any major ground operation, you can also expect to find concentrations of AAA defenses along the FEBA and in-depth to protect forces and command/control nodes. Of course, the larger and slower the aircraft or object, the easier it is to target. AAA pieces are relatively small in size and can normally be easily camouflaged, making accurate visual positioning from the air nearly impossible unless muzzle flashes and/or tracer rounds are seen. It's important to collect all possible information from all crewmembers after a mission that has been fired upon. Only by collecting such tidbits as muzzle flash, rate of fire, tracer color, descriptions of airbursts, smoke, etc, can an accurate assessment of the types, numbers, and importance of active AAA weapons be made.

6.6.2.2.4. Intercept Data. Carefully collect and report all encounters with adversary aircraft. Each report must note the time, altitude, and most importantly, a description of the encounter. On missions where intercepts occur, the extent of air reaction by the enemy indicates their capabilities, strength, and intent. A narrative of the tactics, marking of enemy aircraft, aggressiveness, intensity of the attack, and duration of the encounter are essential to an accurate assessment of the adversary's capability and intent. This data must be reported for any/all intercept activity, regardless of the interceptor's origin.

6.6.2.2.5. Force Protection. During routine peacetime missions, good collection, analysis, and reporting of FP data can make impending threat situations clear and allow employment of mitigating measures to preclude or minimize calamity. Pay close attention to the FP Essential Elements of Information (EEIs) contained in AMCI 14-102, *Intelligence Debriefing and Reporting,* and make every effort to collect and report data that may indicate a threat. Don't accept a "Nothing Significant To Report" (NSTR) debriefing until all the questions have been asked. Sometimes it may have seemed as if there was nothing significant, yet asking the right question may draw out information that, when combined with other reporting, indicates a significant factor.

6.6.2.3. Steps in Mission Reporting. **Chapter 7** of this handbook provides practical information and guidance for conducting debriefings. Debriefing the aircrew is only the first step in fulfilling your post-mission responsibilities. Remember, the debriefing only collects intelligence information about the mission. For this information to be of maximum value, you must report it. While mission, time, personnel, and equipment will determine your unit's actual process, the four basic steps in mission reporting are as follows: are Check and Verify Information, Draft the MISREP, Edit the MISREP, and Disseminate the MISREP.

6.6.2.3.1. Check and Verify Information. In this step you check for possible errors in your information. Do this by cross-checking all items on the debriefing worksheet or checklist against the mission plan and other materials associated with the air operation. Look for items that seem inconsistent or contradictory. As you do this, you may have to consult the debriefer and/or, call the aircrew back for further clarification. Once you've checked over all the information gathered, you are ready to draft the report.

6.6.2.3.2. Draft the MISREP. Create a MISREP shell with pre-mission information, so that completing the MISREPis just a matter of filling in blank spaces. You will receive information that requires you to expand items, and to include new and pertinent mission data. Quite often narrative explanations will be necessary. Keep narratives in the style of a newscast. Provide the "who, what, when, where, and how" of the mission. Record exact coordinates, times, altitudes, and similar details. If the mission data is incomplete or unavailable, state this fact and the reason for it in the report.

6.6.2.3.3. Edit the MISREP. If possible, have a second person read the MISREP prior to transmission. This step can help to ensure discrepancies and/or ambiguities are caught before the information is disseminated to the rest of the community. Key points to review include proper security classification, appropriate terminology and explanations when needed. Double check positions reported, and generally to ensure the report is accurate and complete. Common sense must be applied to this step. Do not delay reporting of critical information for any reason other than accuracy. Minor typographical errors are no reason to make a major ordeal out of the editing process, as long as they don't alter the meaning or accuracy of the information reported.

Do not delay critical reporting for lack of supporting data. Follow-up reporting can always be done at a later time.

6.6.2.3.4. Disseminate the MISREP. Before you disseminate the report, check the distribution list to ensure all appropriate addressees are included. Normally, you should develop reporting templates that have all this data preset to preclude a lengthy process of addressing each report. AMC addressee listings can be found in reporting directives and/or Annex B of the OPORD. Refer to theater directives for guidance on addressees when OPCON has been changed.

6.6.3. Intelligence Report (INTREP). The INTREP provides information regarding events that could have an immediate and significant effect on current planning and operations, or information that may be of timely interest at the higher command levels. Additionally, INTREPS are used to amplify and/or clarify previously reported MISREP information. This message is the primary means of reporting Human Intelligence (HUMINT), counterintelligence information, and INFLTREPs. The INTREP is the primary reporting tool used by unit-level intelligence organizations to report information of intelligence value to lateral, subordinate, and upper-echelons.

6.6.3.1. AMC units may use the online INTREP form provided on the AMC/IN Intelink-S Online forms page at **http://www.amcin.scott.af.smil.mil** unless connectivity is unavailable or you are directed to use other means. Use this form to report significant information obtained through means other than an aircrew mission debriefing. The online INTREP provides a flexible, easy to use format particularly well suited for FP intelligence reporting. The online INTREP form consists of two sections: the Message Header, and the Message Body. All fields in the INTREP must be filled in order for the system to accept the INTREP.

6.6.3.2. You must fill out and submit the message header section before you can enter the body of the report. In the message header, many of the items are selected from scrolling lists. Select the appropriate precedence from the choices of Routine, Priority, Immediate, or Flash. Select the originating agency that correlates to your unit's plain language address. The action addressees are preset by AMC/IN. Don't forget to enter your user id (i.e., 'OSS22') in the classified email block. You must also select an overall report classification. After all these blocks have been filled in, select the number of references pertinent to the report. This action presets the REF and AMPN or NARR blocks on the body of the message. When completed, click "CONTINUE" to proceed to the body section.

6.6.3.3. The Message Body of the online INTREP is fairly simple to accomplish. The system assigns a standard reporting serial number to each INTREP submitted. Reference lines are used to enter specific reference documents, such as an ATO, an OPORD, a previously submitted INTREP or MISREP, or even another intelligence report from another source. The *Amplification* and *Narrative* blocks are free text blocks to describe a specific reference entry (Amplification) or set of multiple reference entries (Narrative.) The full text of the report is entered in the *Remarks* block. Enter a source of classification in the *CLASS BY* block. The *Declassify On date* is automatically set for 10 years from date of submission, but can be changed if warranted.

6.6.3.4. When drafting an INTREP, try to keep it short and to the point while including all significant data surrounding the event or situation being reported. When reporting on a significant event, issue the report as soon as possible. Don't wait for the event to be completely wrapped up prior to issuing the first report. Get the information out as soon as possible and issue follow-up reports to further describe the situation or provide fused analysis of the overall event. What may

seem like an isolated local event could be part of a bigger pattern. Loss of life and damage to resources may be avoided if that pattern is recognized early enough.

6.6.4. Intelligence Summary (INTSUM). While under the OPCON of AMC, units are not expected to produce an INTSUM. If CHOP'd to a theater entity that requires INSTUM reporting, consult that command's reporting instructions for INTSUM reporting procedures and formats.

6.6.5. On-Station Report (OSTREP). The On-Station Report provides AMC/IN with status information on deployed intelligence personnel. These reports are used to ensure deployed personnel have what they need by tracking arrival at deployed location and identifying status of personnel, systems, connectivity, and other requirements. Deployed personnel submit an initial report upon arrival at the deployed location. They issue a follow-up report any time there is a change to the information reported in the initial report. The AMC online OSTREP is located on the Intelink-S Online Forms page at **http://www.amcin.scott.af.smil.mil**.

6.6.6. Off-Station Report (OFFREP). The Off-Station Report is used to report the redeployment of AMC Intelligence personnel. Submit Off-Station reports via the AMC Intelink-S Online Forms page at **http://www.amcin.scott.af.smil.mil**.

6.6.7. After Action Report. The After Action report is an AMC/IN directed report that must be accomplished within two weeks after return from a deployment. This should normally be submitted via the online form available at **http://www.amcin.scott.af.smil.mil**. The information submitted is used to identify problem areas that may require AMC/IN action to correct, as well as processes and procedures that deployed members found effective. When properly completed, this form provides a record for the particular deployment location that can be used by subsequent deployed personnel, somewhat like a turnover briefing. While it's an extensive report, it also offers a "save and continue" function to preclude losing data if the entire form is not completed in one sitting.

Chapter 7

DEBRIEFING

7.1. General. Debriefings are an indispensable tool used by intelligence personnel to extract valuable, time-sensitive information following a mission. Debriefings are not limited to aircrews. They can and should be used to debrief anyone who may have information that affects the organization's mission or the overall operation. Missions or aircraft should be tracked to ensure that they are all properly debriefed. All vital information collected from debriefings should be passed to appropriate agencies and aircrews. This chapter will cover common types of debriefings and some suggestions on how to get the most information in a short time.

7.2. Purpose

7.2.1. The primary purpose of an aircrew debriefing is to obtain information concerning the results of the completed mission. In addition to obtaining mission results, there are a number of secondary purposes.

7.2.2. Thorough debriefings capture information that helps resolve operational issues. The basic information from which we make post-operation analysis and critiques must come from participating crewmembers. This includes recognition and analysis of good and bad procedures in planning and execution. Furthermore, debriefing furnishes information on problems arising from the characteristics of our own equipment.

7.2.3. Debriefing is an important source of first-hand, on-scene intelligence. Pilots and aircrews are often in a position to observe and note "eyes-on" information of the enemy, particularly regarding defenses, massed troops and materiel, tactics employed, etc. This information contributes to time-sensitive targeting and traditional targeting, as well as improves the situational awareness of aircrews, command authorities, and other friendly forces. Your job is to get this information out of the aircrew with as much accuracy and clarity as possible.

7.3. Aircrew Preparation

7.3.1. Preparation prior to mission execution will enhance your unit's effectiveness in debriefing. You must thoroughly train aircrew members in debriefing and reporting, and of their status as intelligence collection resources. Proper training will also make them aware of the importance of the information they collect and how it impacts their safety and the success of future operations. Key avenues to implement this training are local exercises and AIT.

7.3.2. You must carefully develop the interest and competence of flight personnel in debriefing and reporting through training and practice. If aircrew members understand why the intelligence debriefer is asking the questions, what information is essential, and how the information they report is used, they will be more valuable as sources.

7.4. Essential Elements of Information (EEI)

7.4.1. EEIs are critical items of information about the enemy and the battlespace required by the commander and planners to successfully prosecute an operation. Have aircrews review established EEIs and prepare them to observe and report any significant information during debrief.

7.4.2. AMC maintains a standing set of EEIs for day-to-day operations in AMCI 14-102, *Intelligence Debriefing and Reporting*. Combatant Commanders normally maintain their standing EEIs in specific OPLANs and CONPLANS. If your unit is chopping to a theater, make contact with the Air Force element's (i.e. USAFE, PACAF, SOUTHAF, etc) unit support function for assistance in locating the most current EEIs.

7.4.3. Command EEIs can become quite extensive, even overwhelming. You may also discover the need for some elements that haven't been addressed in the command EEIs. You'll need to evaluate the list to determine those items your crews may actually be in a position to observe. This list should then be further tailored and incorporated as an integral part of each pre-mission briefing. If possible, explain to the aircrew why the EEIs being briefed are important. Finally, review the tailored EEIs during the post-mission debriefing.

7.5. Debriefing Challenges.

7.5.1. As a debriefer, you can expect difficulties in your quest for information. In stressful situations, people sometimes find it difficult to clearly observe and comprehend. Observations can be swayed or distorted based upon emotions, perceptions, prior experience, or knowledge. For example, during World War II (WW II), the gunners of the Eighth Air Force claimed destruction of enough aircraft to equal the German Luftwaffe several times over. To avoid reporting false information, you must recognize these tendencies and ensure all information is valid. Objectivity must be the driving goal.

7.5.2. Another problem frequently encountered by intelligence debriefers is dealing with operational terminology. A thorough knowledge and understanding of "ops" terminology can greatly enhance your credibility and the quality of mission debriefings. Know and understand the meaning of terms such as freqs, SPINS, Visual Flight Rules (VFR), etc. Remember, the primary purpose of the mission debriefing is to gather operational information.

7.6. Debriefing Guidelines. Despite the challenges discussed, there are techniques you can develop through study and preparation that will help you obtain the maximum factual information from the aircrew.

7.6.1. Be familiar with the mission. Become familiar with the unit's aircraft capabilities and limitations as well as crew procedures and duties. This can help you talk to the crews in their own terminology and understand what they are telling you. Be familiar with the limitations of aerial observation. Altitude, speed, and weather conditions are obvious deterrents to an accurate observation. Some crew positions may also afford little or no field of view outside the aircraft. The debriefer should know who among the crew is in the best position to observe in any given direction.

7.6.2. Be analytical. The questions you ask must help solve problems, including those that become evident as the debriefing progresses. Much of this effort involves remaining focused on the overall situation being debriefed, critically evaluating information received, and assigning meaning to that information with regards to what was previously known and assessed.

7.6.3. Guide the discussion. You must control the discussion to prevent it from straying off to irrelevant objectives. You must know when to pursue a current line of questions and when to move on to the next subject. You must also be sensitive to information offered that may not seem appropriate for the immediate question, but may still be significant.

7.6.4. Be patient. Most AMC missions are in the air for many hours and cover thousands of miles resulting in physical and mentally exhausted aircrew. Understand and adjust to the emotional state of the crew.

7.6.5. Identify items of importance. Despite a written record of the important items during debriefing, the significance of some things may not be clear at that moment. A good debriefer can associate observations from many different discussions and build an analytical picture, realizing the significance of information that might otherwise be overlooked.

7.6.6. Hunt for facts. While the information reported may be true, if it doesn't appear to mesh, then that is probably significant in its own right. If something doesn't sound right or isn't "adding up" to what was previously known, delve further into the subject and root out the facts that either prove or disprove it. It's up to you, as the debriefer, to draw out and assimilate the facts.

7.6.7. Know the aircrew's priorities. Always keep in mind that an aircrew's primary purpose is to fly the aircraft, conduct the mission, and return safely to base. Observing and reporting are functions incidental to this primary purpose. Do not expect aircrew members to accomplish their complex assignments and devote a great amount of time to observing and recording intelligence information.

7.7. Debriefing Preparations. As previously stated, most AMC missions cover many hours and thousands of miles. By the time the crew returns, they may be running out of crew-duty-day. There are things you can do to maximize the effectiveness of your debriefing session while also minimizing the amount of time it takes.

7.7.1. Preparation for debriefing should begin as soon as the pre-mission briefing concludes. Much of the preliminary information on any debriefing form (mission number, call signs, crew names, target/objective, etc.) can be filled in prior to return of the mission crew.

7.7.2. When appropriate, assemble visual debriefing aids ahead of time. These may include threat recognition guides, target/objective area imagery, charts, etc.

7.7.3. Study the OB and situation displays to know what you can logically expect the aircrews to see.

7.7.4. Make the debriefing area as comfortable as possible.

7.7.5. Monitor landing times to ensure all appropriate debriefings take place and that no time is wasted.

7.7.6. If in-flight reporting was accomplished, gather as much information about the mission as possible.

7.7.7. There may be occasions when you'll have to support "quick-turns," such as Engine Running On/Offloads (EROs) or drop-and-go transient crews. You may be conducting a debriefing and a pre-mission briefing at the same time. These situations don't allow much preparation time, so ensure you have defined and practiced procedures in place to handle them before they occur. Additionally, ensure procurement of safety gear (ear protectors, reflective belts) has been accomplished flight line training has been provided.

7.8. Develop Debriefing Checklists. A good debriefing checklist can be your most valuable aid for conducting debriefings. There is no standard Air Force debriefing checklist; however, all operational units use a debriefing checklist of some type, usually one devised locally. Depending upon the type of mission, some may be simple one-page forms, while others are multiple pages in length. Whatever type of debrief-

ing form you use, it should aid you in getting the information you will need for reporting the mission results and observed items of intelligence interest. Provide a copy of your debriefing checklist to the crew during the pre-mission briefing so they can take it on the mission with them. It will aid the crew in remembering significant activities and help speed the debriefing process. A sample debriefing checklist/form is provided at the end of this chapter.

7.9. Debriefing Procedures. There are a number of rules that apply to debriefings, regardless of the kind of mission or aircraft involved. When you conduct a debriefing, it is important you follow these rules:

7.9.1. Be aware that you're not the only person with whom the crew must debrief. They normally must debrief with maintenance and possibly the mission planners and tactics folks. All of these issues compete for limited available time at the end of a long mission or between missions. It is critical to complete the intelligence debriefing as quickly as possible.

7.9.2. You must obtain all observations while they are still fresh in the minds of the participating aircrew members. The longer the delay, the greater the opportunity for facts and specifics to become distorted or forgotten.

7.9.3. Exclude all unnecessary and unauthorized personnel from the debriefing, and keep distractions to a minimum. Preferably debrief the aircrew in a separate room or enclosure away from other aircrews and debriefings.

7.9.4. Make all basic reference materials, such as charts and photographs used in planning the mission, available at the debriefing table. These items greatly aid in producing definitive and specific information.

7.9.5. Do not criticize or contradict the crew. Expect inaccuracies in their observations. Use facts to validate or disprove claims without injecting personal evaluations. Remember that you have no firsthand knowledge of what the crew did or didn't observe.

7.9.6. Accomplish debriefings quickly, accurately, and tactfully. The information should be precise and answer questions of what, when, where, and how.

7.9.7. If you filled out any information on the debriefing checklist ahead of time, have the crewmembers review it to ensure accuracy.

7.9.8. No matter how elaborate the debriefing checklist, it can serve only as a guide to the debriefer. You need to develop the mental flexibility necessary to recognize information that may be of the highest significance, even if it's not asked for on the form.

7.9.9. Avoid asking leading questions. Don't hesitate to ask additional questions or to aid the crewmember to describe something if it required further explanation.

7.9.10. Try to get aircrew members to participate. Often the least talkative members are the best observers.

7.9.11. While every effort should be made to do so, it may be impossible to debrief all crews the moment they touch down. If possible, provide a comfortable area where crews can wait, but you must keep waiting to an absolute minimum.

7.10. After the Debriefing. Upon completion of the debriefing, ensure it is properly classified and is handled as such. In addition, there may be circumstances that necessitate calling an aircrew back to obtain

additional information. Always ensure you have the approval of unit leadership if it's going to impact crew rest.

Classified _____ When Filled In

Debriefer: _____

Phone: _____

AMC/IN DEBRIEFING CHECKLIST
ITINERARY

Mission Number:	Mission Type:	SQ/ACFT/MSN CC:	Call Sign:
Destination: Track/LZ/ DZ	Arrival DTG/TOT:	Departure DTG:	Aircraft: Number and Type

Ingress WX:	Target Area WX:	Egress WX:	***MISSION RESULTS*** Successful Unsuccessful Remarks:

SIGNS OF DOWNED AIRCREW

Type: (beacon, chute, flare...)	Location:	Remarks:

ENCOUNTERED THREATS

Hostile Aircraft	YES	NO	Remarks:
Hostile SAMs	YES	NO	Remarks:
Hostile AAA/Gnd Fire	YES	NO	Remarks:
Naval Sightings	YES	NO	Remarks:
Ground Sightings	YES	NO	Remarks:
Lasing/Spotlight Incident	YES	NO	Remarks:
Spectrum Interference Resolution (SIR) (formerly MIJI)	YES	NO	Remarks: Remind crew of operations channel report requirement IAW AFI 10-707

EEIs ASSIGNED and RESPONSE

EEI Number	Description/Response

HOSTILE AIRCRAFT ENCOUNTERED
YOUR AIRCRAFT

Location (Lat/ Long):	Heading:	Altitude:	Speed:
C2/ABCCC Acquired	AWACS/Gnd Radar Acquired	Visually Acquired	Time of Sighting:
Hostile aircraft relative position to your aircraft at time of sighting:			

HOSTILE AIRCRAFT

Number/Type:	Heading:	Altitude:	Speed:	Formation:
Missiles Fired (type and number):	Guns Fired:		Time of Engagement:	
Direction of Approach:	Use of Afterburner:		Any Reattack:	
Color Scheme of Aircraft:		Markings Observed:		

YOUR EVASIVE MANEUVERS/COUNTERMEASURES AND EFFECTIVENESS

BATTLE DAMAGE OR LOSSES

EFFECT OF INTERCEPT ON MISSION

HOSTILE SAMs ENCOUNTERED

YOUR AIRCRAFT

Location (Lat/Long):	Heading:	Altitude:	Speed:
Time of Sighting:	When Acquired: (at launch or in air)	How Acquired: (visual, ADS, RWR...)	Confirmation:

HOSTILE SAM

Site Configuration:		Type/Number of Missiles Launched:	
Size of Plume: (Compared to Missile)	Color of Plume:	Type of Contrail:	Missile Size:

DETONATIONS OBSERVED

Number:	Color:	Altitude:	Miss Distance:	Relative Position to ACFT:

EVASIVE MANEUVERS EMPLOYED - EFFECTIVENESS

COUNTERMEASURES EMPLOYED

REACTION OF SAM TO COUNTERMEASURES

BATTLE DAMAGE OR LOSSES

EFFECT OF SAM ON MISSION

HOSTILE AAA/GROUND FIRE ENCOUNTERED

YOUR AIRCRAFT

Location (Lat/Long):	Heading:	Altitude:	Speed:	Time of Engagement:

HOSTILE AAA/GROUND FIRE

Weapon Location:	Type/Number of Weapon:	
Light fire (1-5 rounds):	Medium Fire (15-30 rounds):	Heavy Fire (30-plus rounds):
Muzzle Flash Color:	Number of Airbursts:	Color of Airbursts:
Altitude of Airbursts:	Tracer Color/Time Interval:	Accuracy of Fire:
Relative Position of Airbursts to Aircraft:	Closest Miss Distance:	
Radar Associated:	Other Aircraft Affected:	

EVASIVE TACTICS EMPLOYED AND EFFECTIVENESS

BATTLE DAMAGE OR LOSSES

EFFECT OF AAA/GROUND FIRE ON MISSION

NAVAL FORCES ENCOUNTERED

YOUR AIRCRAFT

Location (Lat/Long):	Heading:	Altitude:	Speed:
Time of Sighting:	When Acquired: (at launch or in air)	How Acquired: (visual, ADS, RWR...)	Confirmation:

TYPE AND NUMBERS OF VESSELS

Time of Sighting:	Location of Sighting:	Nationality:

Aircraft Carriers (Helicopter Carriers):	Major Surface Combatants (Cruisers, Destroyers, Frigates...):
Minor Surface Combatants (Patrol Boats):	Auxiliaries and Non-Combatants:
Submarines:	Speed and Heading of Ships:

REACTION OF SHIPS TO YOUR AIRCRAFT

FIGHTER COVER PROVIDED

Time to intercept:	Location of CAP:	Type/Number of Aircraft:
Aircraft Configuration:	Markings/ Colors:	Tactics:

ADDITIONAL REMARKS

GROUND FORCES ENCOUNTERED

YOUR AIRCRAFT

Location (Lat/Long):	Heading:	Altitude:	Speed:
Time of Sighting:	When Acquired: (at launch or in air)	How Acquired: (visual, ADS, RWR...)	Confirmation:

GROUND SIGHTING

Location:	Number of Troops/Vehicles:	Did You Receive Fire?

TYPES OF TROOPS SIGHTED

Infantry:	Armor:	Artillery:	Other:

TYPES OF VEHICLES SIGHTED

Tracked:	Wheeled:	Trailers:

STATUS

Static:	Dug-in:	Moving (note direction):

TERRAIN (Check all that apply)

Flat:	Hilly:	Forest:	River Crossing:	Mountainous:

ELECTRONIC SITE

Antennas (type/number):	Status (Temp or Perm):	Vehicles (type/number):

AIRFIELD

Status (active, useable...):	Runway Length:	Runway Width:	Defenses:
Runway Construction (Dirt, Concrete, Asphalt...):		Runway Orientation:	
# Small Hangars:	# Medium Hangars:	# Large Hangars:	# Bunkers:
POL Location:		Ammunition Storage Area:	

ADDITIONAL REMARKS

LASING/SPOTLIGHTING INCIDENT ENCOUNTERED
YOUR AIRCRAFT

Location (Lat/Long):	Heading:	Altitude:	Speed:

LASING/SPOTLIGHTING SOURCE

Time of Incident	Relative Position	Geo Position	Duration Of Incident
Color of Light	Focus (Spot, Flood, Pin)	Behavior (Scan, Track, etc)	Exposure Impact/ Damage

ADDITIONAL REMARKS

SPECTRUM INTERFERENCE ENCOUNTERED

YOUR AIRCRAFT

Location (Lat/Long):	Heading:	Altitude:	Speed:

SPECTRUM SOURCE

Time of Incident:	Spectrum Affected: RADAR, IR, VHF, UHF, FM	Percent Effective:	Duration Of Incident:	
Type: Voice/Static/Beep	Mission Impact:	Crew Response:	AWACS Notified: Y/N	Freq. Affected:

ADDITIONAL REMARKS

Chapter 8

SYSTEMS AND COMMUNICATIONS

8.1. General. AMC's rapid mobility requirements and the global nature of AMC operations drive the need for a scalable, and flexible Intelligence Information Systems (IIS). The AMC IIS provides a 21st century systems infrastructure by leveraging advances in Commercial Off-the-Shelf (COTS) and Government Off-the-Shelf (GOTS) hardware, software, and communications technologies. AMC/IN has integrated a host of capabilities into a collaborative environment allowing intelligence analysts, producers, and operators to perform collaborative mission planning anywhere in the world. They can simultaneously work on documents or briefings, exchange information, perform research, and analyze imagery or other intelligence information from even the most austere forward operating location.

8.2. AMC Intelligence Information Systems. The AMC/ISS is the culmination of the AMC Intelligence Collaborative Environment (ICE) migration effort, which moved AMC Intelligence to a cost-effective personal computer (PC) architecture. The AMC/IIS provides many positive administration, operations, and maintenance benefits when compared to previously fielded systems.

8.2.1. In-garrison users meet the challenges of FP intelligence with networked desktop and/or laptop PCs connected to a local area network (LAN) with connectivity to Secret Internet Protocol Router Network (SIPRNET). Deployed intelligence operations are met with laptop PCs connecting to SIPRNET via the host base or the AMC Intelligence reach back communications facility, which is discussed in greater detail in para. **8.2.** below.

8.2.2. The majority of AMC unit-level FP and intelligence information requirements are satisfied with products stored on the AMC Intelink-S server. Unit-level intelligence professionals can access products and services with nothing more than an industry standard web browser secure SIPRNET connectivity.

8.2.3. AMC/IIS helps reduce the subordinate unit system administration burden by providing "centralized" technical support from the AMC Intelligence System Branch (AMC/INYS). The AMC IIS centralizes mail, database, web, collaboration, near-real time and other critical servers at the headquarters level where the systems support expertise resides. All hardware components are purchased with extended warranties, thereby eliminating the need for each unit to set aside funds for maintenance.

8.2.4. Near-Real-Time (NRT) Threat Information. Access to national and theater-level NRT intelligence is provided via a web browser or by connecting to the AMC/IN NRT server, which rebroadcasts the information over SIPRNET for Falcon View users. This negates the need for each unit to maintain Tactical Receive Suite (TRS) to access the Tactical Information Broadcast System (TIBS), and Tactical Receive Applications (TRAP). SIPRNET users can access the AMC NRT archive fro the AMC Intelink-S server. Falcon view users can access a live feed by connecting to **207.84.25.122** Port 4000, as a client.

8.2.5. Falcon View. The Falcon View component of the Air Force Portable Flight Planning Software (PFPS) provides geospatial, mission planning, NRT feed, order of battle (OB), and threat analysis capabilities for AMC intelligence. Falcon View can display standard NIMA-produced digitized map/chart files in (Compressed Digitized Raster Graphics (CDRG)) Controlled Image Base (CIB), and Digital Terrain Elevation Data (DTED) formats. User-produced situation and mission are overlaid

onto digital mapping products. Using the NRT "broadcast repeater" function described in para 8.1.4 above, NRT threat data can be automatically plotted and displayed, providing a continuously updated threat picture.

8.2.6. Collaboration Tools. Members of the extended AMC Intelligence family can collaborate together in a virtual workspace to overcome barriers of distance and time. Microsoft NetMeeting provides a cost effective collaboration tool that supports application sharing, desktop Video-Tele-Conferencing (VTC), user-friendly file transfers, analyst-to-analyst chat functions, and a shared whiteboard. NetMeeting provides access to the AMC Intelligence Conference Server which can support a "virtual meeting" of up to 25 different locations.

8.2.7. AMC Intelink-S Server. The AMC Intelink-S server provides "one stop Shopping" for critical FP and intelligence products and service officered by AMC/IN and the AMC Threat Working Group (TWG). The following paragraphs describe the major capabilities offered on the AMC Intelink-S Server.

8.2.7.1. On-Demand Order of Battle. Supports the creation of preformatted order-of-battle (OB) reports (e.g. air, defensive missile, electronic, ground, and naval) and allows users to extract OB information in formats friendly to intelligence, mission planning, Geospatial Information Systems (GI&S), databases, spreadsheets, etc. The On-Demand OB directly connects to the USTRANSCOM Modernized Intelligence Data Base (MIDB) and is available from the AMC Intelink-S server.

8.2.7.2. General Military Intelligence (GMI) Gateway. Provides critical infrastructure information (installation, facilities, unit, equipment) directly from MIDB-S with nothing more than a web browser. Provides preformatted reports and extracts in a format friendly to mission planning, intelligence, databases, and other systems.

8.2.7.3. Virtual Threat Assessor (VTA). Delivers global FP knowledge management to the AMC TWG, enabling it to determine threats to AMC/USTRANSCOM assets at all transportation facilities worldwide. Received the DoD 2000 Anti Terrorism/Force Protection Innovation Award.

8.2.7.4. Virtual Risk Assessment Database (VRAD). Automates the research, creation, coordination, and dissemination of AMG TWG airfield risk assessments. Contains "formal" airfield risk assessments produced by the AMC TWG.

8.2.7.5. Digital Isolated Personnel Report (ISOPREP) System. Allows unit intelligence personnel to create, manage, and electronically deploy digital ISOPREP cards for flying personnel assigned to their unit.

8.2.7.6. Global Terrorism Database. Provides all-source information on domestic and transnational terrorist groups and the acts they commit.

8.2.7.7. AMC/IN Debriefer. Extracts information of intelligence or FP

Interest from aircrews and automates the preparation of Phoenix Raven airfield security surveys.

8.2.8. Phoenix Resource. Phoenix Resource is the AMC/IN intranet that provides a single point-of-entry database that streamlines reporting and analysis of unit readiness information. It allows unit leadership to track personnel and their qualifications, equipment inventories, and deployment commitments. For AMC HQ and Units, Phoenix Resource is a resource that provides a "snapshot" of any unit's intelligence capabilities, shortfalls, and readiness.

8.3. Communications. Without a means to exchange data, or to communicate, the best automation provides little practical benefit. The AMC/IN Systems Integration Management Office (SIMO) identified a command requirement to exchange information and coordinate issues between all levels of command horizontally and vertically. Effective secure data communication requires connectivity to SIPRNET. The AMC Intelligence System Architectures meet this connectivity requirement via several different means, including dedicated hardwire connectivity, the Quick Dial-Up Capability (QDUC), its follow-on the Remote access secure Program (RASP), and the Deployable Intelligence Support Kit (DISK).

8.3.1. Secret Internet Protocol Router Network (SIPRNET). SIPRNET is the common communications thread interconnecting the intelligence producer and the warfighter. In-garrison direct access to SIPRNET is essential for every AMC Intelligence work center. Over the past several years, AMC/INY has installed, or assisted in the installation of SIPRNET at most AMC and AMC-gained unit for in-garrison use. AMC/INY has also provided multiple means to access SIPRNET when deployed, or when primary circuits fail. The QDUC, RASP, and DISK make secure "reach back" communications capability possible. Information and procedures in operating these systems are available on the AMC/IN SIPRNET Homepage (**https://www.amcin.scott.af.smil.mil**) under “Support.”

8.3.2. Quick Dial Up Communications (QDUC). QDUC provides basic dial-up access to SIPRNET and critical intelligence servers and services located at AMC Intelligence and across the Department of Defense (DoD). QDUC operates like a secure version of the Internet Service Provider (ISP) you probably use at home. The AT&T model 1900 or 1910 Secure Data Devices (SDDs) provide a secure, encrypted linkage between the unit’s PC and a phone-line connection to the AMC/IN Intelink-S servers (DSN 576-3575/8428, Comm (618) 256-3575/8428). QDUC connection speeds are limited to 9.6 KiloBits Per Second (kbps) with the AT&T 1900, and 38.4 kbps with the AT&T Model 1910.

8.3.3. Remote Access Secure Program (RASP). RASP is the replacement for QDUC , a legacy system. Mykotronx Palladium (secure modem) provides faster and more error-tolerate access to SIPRNET for deployed personnel. The Palladium secure modem is a PCMCIA card that fit in any “type a” PCMCIA slot. All laptop computers and some desktop systems have this slot as standard equipment. Together with the Personal Identification Number assigned by AMC/INYS the system can dial-in to AMC/IN’s telephone banks at a baud rate significantly higher than the QDUC SDD-1910 system (33.6Kps).

8.3.4. Deployable Intelligence Support Kit (DISK). DISK provides worldwide access to SIPRNET from austere locations. DISK differs from QDUC in that it does not require a phone line to operate. QDUC utilizes a commercial International Maritime Satellite Model -B (INMARSAT-B), Cisco router, laptop PC, and Allied Signal KIV-7 encryption device to access SIPRNET. DISK transfer rates are higher than QDUC (64kbps vs. 38.4kbps); however, there is a $9.00 a minute connection fee associated with DISK. DISK should only be used in areas where there are no other means to connect to SIPRNET.

8.3.5. IRIDIUM. Iridium phones allow anyone to make a secured or unsecured phone call from virtually anywhere in the world. Each phone is designed and sent with a specially configured Subscriber Identity Module (SIM) Card. The SIM card contains personal international phone numbers (similar to PINs), account information (user organization, etc.), and allows user to store frequently dialed numbers. These cards have the unique ability to be transferred to any Iridium phone and continue to maintain their identity as well as permit the user to universally send and receive calls. This system is not meant to replace the current DISK system, but merely to augment voice capability as well as reduce costs. At this time, there are no plans to allow data connections (laptops).

8.3.6. Messaging. A Secret/NOFORN messaging capability is provided by Defense Message System (DMS), which has replaced Automatic Digital Network (AUTODIN). Intelligence units should ensure they have established a DMS address with their local Communications Squadron to ensure they received required message traffic.

8.3.7. Electronic Mail. AMC/IN supports the transfer of secure electronic mail (e-mail), which is used as the primary method for communications and coordination. AMC Intelligence maintains a mail server (mail.amcin.scott.af.smil.mil) for AMC units. The reliability of secure electronic mail is degraded when QDUC users attempt to pass large files (usually 700k or larger). This is caused by the relatively slow transfer rates experienced by Quick Dial up Capability (QDUC) and RASP users. Recommend telling the people you exchange email with about this limitation to avoid problems.

8.4. Useful On-Line System References: For further information on AMC Intelligence Systems, please visit the systems support section or the AMC/IN Virtual University on the AMC Intelink-S Server.

Chapter 9

INSPECTIONS, ASSISTANCE, EXERCISES

9.1. General. The HQ AMC Inspector General (IG) manages the command's readiness inspection program IAW AFI 90-201, *Inspector General Activities*, AMCI 90-201, *The Inspection System*, and AMCP 90-202, *Inspection Guide*. In addition, HQ AMC/IG is also responsible for intelligence adherence to Intelligence Oversight as outlined in AFI 14-104. HQ AMC INXU conducts intelligence unit Staff Assistance Visits (SAV) on active duty units to assist in trouble-shooting problems and fine tuning daily operations. Active duty units will normally be scheduled to receive a SAV every other year. ANG and AFRC units can request a SAV in preparation for a scheduled AMC ORI. This request must be coordinated between the IN/Intel OIC and AMC Unit Support. SAVs to ANG and AFRC units will be unit funded.

9.2. Mission Essential Task List (METL).

9.2.1. As defined in AFDD 1-1, *Air Force Task List*, a Mission Essential Task (MET) is a task selected or expanded on from the Air Force Task List (AFTL) as a fundamental requisite for the performance or accomplishment of an organization's assigned mission. At the lowest organizational levels, METs are those critical tasks that must be accomplished to effectively meet UTC mission requirements. A "METL" is nothing more than a listing of all METs applicable to a specific unit or command.

9.2.2. Development of a unit METL is the first step in building a true requirements based training plan. The unit's training plan must then provide a credible plan for use in training unit members to consistently and accurately accomplish those mission essential tasks.

9.2.3. AMC has defined a set of common, command-wide, unit-level METs and disseminated them via the "AMC Unit-Level Mission Essential Tasks Version 3.0," dated 1 Jan 03. Because this list is only written down to the squadron level, there is only one purely "intelligence" task presented. The following extract presents AMC Unit-Level Mission Essential Task 3.05.01.

3.05.01. Provide Timely, Integrated, All-Source, Intelligence Support to Leadership, Mission Planners, Flying Squadrons, and Base Operating Support Functions Through All Phases Of Unit Operations.

Provide fused, all-source actionable intelligence analysis and dissemination of military/ geo-political situations impacting current and planned unit operations. Provide near-real-time analysis and dissemination of adversary force disposition, capabilities, and intentions impacting employment operations. Provide intelligence input to mission planning and aircrew preparation for combat employment missions, to include route threat assessment, evasion and recovery planning support, pre-mission intelligence briefing, and post-mission debriefing and reporting. Conduct battle-space analysis, develop unit-level intelligence estimate of the situation, and disseminate estimates/updates to unit leadership and lateral/subordinate units and personnel (including Base Operations Support personnel, transient aircrews/personnel/units, and CRAF/ .Contractual carriers). (HQ AMC/INX)

9.2.4. The accompanying standards define the criteria and measures to be used in determining the unit's success in accomplishing this mission essential task.

STANDARDS CRITERIA / MEASURES			
M1	80	Percent	Of UTC-tasked intelligence capabilities (personnel and equipment) maintained in deployment/mission ready status.
M2	8	Hours	Status/shortfalls of UTC-tasked intelligence capabilities will be reflected in Phoenix Resource.
M3	100	Percent	Of tasked intelligence resources palletized and delivered to transportation for joint inspection, marshalling and deployment IAW deployment order and installation/ unit Deployment Schedule of Events.
M4	100	Percent	Of intelligence equipment and personnel accounted for through all phases of operations.
M5	100	Percent	Of pertinent intelligence information acquired, analyzed, tailored to unit/mission needs, and disseminated to appropriate audience through all phases of operations.
M6	2	Hours	Prior to departure, deployed non-aircrew personnel briefed on general situation generating deployment and threats to operations/forces at secure launch or Phoenix Raven required deployment locations.
M7	2	Hours	Personnel ready to brief deployed non-aircrew personnel on general situation generating deployment and threats to operations/forces at non-secure launch or non Phoenix Raven required OCONUS deployment locations.
M8	100	Percent	Of deployment mission aircrews provided with Deployment Mission Intelligence Briefing per command guidance/theater direction prior to departure.
M9	24	Hours	After arrival at deployed location to set-up intelligence operating location and establish flow of secure and non-secure information.
M10	24	Hours	Intelligence operating location established providing flow of secure and non-secure information; make contact with nearest AMC En Route Intelligence Unit.
M11	100	Percent	Of tasked employment missions provided with combat intelligence support for mission planning and aircrew preparation (mission threat analysis and pre-mission briefing).
M12	15	Minutes	Disseminate critical/perishable force protection threat information to key leadership and initiate activation of local Threat Working Group or like function.
M13	1	Hour	Provide information to key leadership and/or TWG or like function.
M14	4	Hours	Disseminate non-critical force protection threat information to key leadership and/ or TWG or like function.
M15	4	Hours	Convene TWG, develop local area threat assessment, and disseminate non-critical force protection threat information to key leadership.
M16	2	Hours	Disseminate mission results and items of intelligence value collected via post-mission debriefing per command/theater spins.
M17	95	Percent	Provide recurring training to aircrews on threats, their lethality, and avoidance techniques.
M18	100	Percent	Of ISOPREP maintenance of aircrew from Geographically Separated Units (GSUs), home station units, and tenant organizations (HQ AMC and USTRANSCOM)

9.2.5. To augment the AMC Unit-Level METL and provide units with a more comprehensive standard, HQ AMC/INX has developed a supplementary task list. This list, titled *Intelligence Task List* (INTL), is published as attachment 3 of AMC Supplement 1 to AFI 14-105, *Unit Intelligence Mission and Responsibilities*. As part of a supplement to an Air Force Instruction, it is directive.

9.2.5.1. In the INTL, items numbered 1 through 11 and printed in bold type denote critical Intelligence Tasks (INTs). INTs are those critical supporting tasks that must be accomplished in order to fulfill the single mission essential intelligence task (3.05.01) listed in AMC Unit-Level Mission Essential Task. Each INT is further broken down to define subordinate tasks that must be accomplished in order to meet INT standards.

9.2.5.2. The INTL provides a fairly generic standard that can be applied command-wide. Each intelligence flight/element must use this list as a baseline to begin building its own tailored, unit-specific task list. In doing so, the unit not only defines those tasks critical to mission success, but also defines the essential core for an effective requirements-based training plan. For additional guidance and assistance in developing a unit-specific task list and training plan, refer to these additional AMC documents:

HQ AMC Joint Training Plan - updated 16 Feb 2000, is available at
https://amc.scott.af.mil/do/dop/downloads/amcjtp9902v4final.doc

HQ AMC Joint Mission Essential Task List, updated 11 Jan 2000, is available at
https://amc.scott.af.mil/do/dop/downloads/JMETLV4Final.doc

9.3. Inspector General. In this portion of the handbook, we'll examine why AMC has an inspection and assessment system, briefly explain the Expeditionary Operational Readiness Inspection (EORI) process and grading methodology, what to expect during an inspection, and how to best prepare for it. Helping units achieve a high state of readiness and mission accomplishment are endgame IG objectives.

9.3.1. Why do we need an inspection system? Global hotspots demand that we, as a trained fighting force, be prepared to deploy at a moment's notice to defend US and ally resources and interests worldwide. Integral to that aim is our requirement to effectively and efficiently "pack up and go." The IG Inspection System is designed to assess the capability of units within the command to perform their missions and to provide feedback to HQ AMC, NAF, and unit commanders. Honest evaluations and results reporting are the vehicles used to objectively assess an organization's readiness state and ability to respond to any worldwide crises.

9.3.2. Expeditionary Operational Readiness Inspections.

9.3.2.1. The basic goal of HQ AMC-directed inspections, as stated above, is to provide commanders with realistic evaluations of how well their forces can accomplish wartime missions. However, 3rd quarter 1999 brought about fundamental changes to the HQ AMC IG inspection process. Specifically, the IG adopted the EORI CONOPS to better mirror the Air Force's shift to a contingency-oriented, UTC based, "rainbow" fighting force — the Expeditionary Aerospace Force (EAF). The days of a "one base fighting force" are virtually gone.

9.3.2.2. There are two types of EORI inspections: IG-Generated Exercises (IGX) and demonstrated operational capability inspections – which are direct observations of real-world operations (AEF deployments, CJCS Exercises, contingency operations, significant Joint Airborne/Air Transportability Training (JA/ATTs), and other opportunities to evaluate identified UTCs in a real-world (or simulated) environment. A mix of inspection types offers a better picture of overall command readiness than the traditional one shot, single wing inspections of the past.

9.3.2.3. It's important to understand that the AMC staff directorates (e.g., IN) develop the inspection criteria (METs) used by the IG to evaluate unit readiness. These criteria reflect the commander's priorities to ready their forces from mission preparedness to mission accomplishment. The IG uses these criteria as a guide to provide a realistic assessment of a unit's mission capabilities. The bottom line is, the IG team does not make policy; it evaluates and enforces the commander's policy.

9.3.3. The EORI Process. During an EORI, the IG team evaluates four distinct categories of unit readiness (formerly known as major graded areas): Initial Response (IR); Employment; Mission Support; and Ability to Survive and Operate (ATSO).

9.3.3.1. Initial Response. All deployment actions a unit accomplishes in preparation to get passengers and/or cargo to where they're needed.

9.3.3.2. Employment. Employment involves the safe delivery of passengers and/or cargo. Inter- and intra-theater missions may include air-land, aerial delivery, aerial refueling, aeromedical evacuation, and other unique missions.

9.3.3.3. Mission Support. Critical to the employment phase, mission support facilitates mission accomplishment and directly affects the unit's ability to perform its wartime mission.

9.3.3.4. Ability to Survive and Operate (ATSO). ATSO is the integrated employment of all components of the airbase to ensure the installation and its forces are capable of sustained mission success in a hostile environment.

9.3.4. Grading.

9.3.4.1. IG inspectors use AMCP 90-202, *Operational Readiness Inspection Guide*, criteria to assign grades to mission essential and supporting tasks. These task grades are ultimately used to "color" the UTC grade, and determine the readiness state of that UTC.

9.3.4.2. In relation to EORIs, the IG adopted a revised "stoplight," color-based methodology of assigning ratings to assorted performance standards required for successful task accomplishment. These "stoplight" colors and their meaning are: **GREEN = "mission ready**," **LIGHT GREEN = "mission ready with comments that require action or attention," RED = "not mission ready," and BLUE = "not observed."**

9.3.4.3. IG members will assign grades based on direct observation of applicable measures or tasks performed. Many of these direct observations will take place during actual unit mobilizations or deployments.

9.3.4.4. Intelligence plays a significant role in each of the four readiness categories and the overall assessment your unit will receive. The primary wartime intelligence functions/processes performed at various times throughout the ORI are Support to Aircrews, Support to the Commander and Staff, Support to Deploying Support Personnel, Mobilization and Deployed Operations, Data-

base/Information Management, Personnel Management, Debriefing and Reporting, Effective Use of Automated Equipment, and Reachback.

9.3.4.4.1. Support to aircrews. This should probably be your number one concern, and should emphasize mission planning, threat awareness, and integration with tactics. The desired result of this process is to enhance aircrew survivability and mission success through a clear understanding of all potential threats to unit air operations.

9.3.4.4.2. Support to the Commander and Staff. Ensure key decision makers receive timely tailored intelligence on all events impacting their units and all potential threats to their operations. The desired result of this process is an informed command staff capable of making the appropriate decisions to support the mission and protect resources.

9.3.4.4.3. Support to Deploying Support Personnel. These personnel require a concise tailored briefing on the situation and potential/actual threats at the forward operating base. The result of this process is an informed cadre of personnel who understand the situation and the threat in the area they are deploying to.

9.3.4.4.4. Mobilization and Deployed Operations. The requirement to mobilize and provide deployed support varies significantly depending on the unit mission. The inspector will observe and assess units with a mobility/deployed operations mission on their ability to deploy appropriate personnel and equipment and establish effective support to deployed operations. The result of this process should be the rapid and effective establishment of deployed intelligence support at the Forward Operating Locations (FOLs).

9.3.4.4.5. Data Base/Information Management. Effective document/information management is critical to your ability to support your customers and mission success. This includes the effective use of local resources, the timely integration of scenario intelligence into your briefings, timely requests for information/imagery from outside your unit, and a clear understanding of what your unit is doing and when it will do it. Your ability to perform this process will directly impact on the support you provide to the mission. The focus is to provide timely, tailored mission essential information to your customers. Internally, your office will need a process to manage the flow of intelligence and mesh it with what your unit is tasked to do. Good changeover briefings are essential to this process. The result should be an office that is fully aware of what its unit is doing, and that it provides timely, tailored intelligence to support the customer and mission.

9.3.4.4.6. Personnel Management. This process may vary depending on your resources and tasking. Depending on your situation, you may need to request augmentation from local units or the MAJCOM. If you require augmentation, prepare to rapidly integrate these personnel into your operations. The desired result of this process is to ensure you have enough trained personnel available to provide effective intelligence support to your customers and the unit's mission.

9.3.4.4.7. Debriefing and Reporting. These requirements are consistently an area of confusion. The best advice is to aggressively follow guidance in the most current AMCI 14-102, *Debriefing and Reporting*. The IG team will thoroughly evaluate your ability to quickly and accurately perform reporting functions such as MISREPs and INTREPs.

9.3.4.4.8. Effective Use of Automated Equipment. This area has grown significantly in importance to successful intelligence operations over the past few years. Effective use, deployment,

and setup of all automated equipment are issues of high priority to HQ AMC/IN. Make every effort to maximize use of all homestation or deployed automated equipment to facilitate dissemination of critical intelligence information to aircrews, commanders and staff, and support personnel immediately. In an IGX environment, IG inspectors may require specific actions and/or specific information from your unit's homestation or deployed automation equipment.

9.3.4.4.9. Reachback. Deployment to another location should not/does not eliminate your contact with homestation personnel. Regardless of how much advance preparation that goes into an upcoming deployment, no mobilization is perfect. Certain intelligence support may/will be required from homestation or command-level intelligence personnel not located in theater. Requesting this support is known as Reachback. Reachback done either electronically via automated systems or via telephone is critical to continued intelligence support to the deployed warfighter.

9.3.5. Validation.

9.3.5.1. At the conclusion of an EORI, the intelligence evaluators will typically out-brief the Senior Intelligence Officer, or their designated representative. The SIO may elect to include other key unit members as appropriate. Recall from the Grading section that the IG relies on direct observation of several performance tasks. Observations of your unit's performance on these tasks are primarily what are discussed. This is where the "good, the bad, and the ugly" come out. The overall unit report, validated by the EORI Team Chief with your wing or group commander, can include strengths and will include areas for improvement.

9.3.5.2. A unit readiness assessment is the immediate result of an EORI. However, an equally important result is the identification of unit strengths and weaknesses and the quality of support provided by higher headquarters. IG inspectors will brief these observations to HQ AMC/IN and staff following the EORI. HQ AMC/IGPO will also track items and issues requiring action by the headquarters staff.

9.3.6. EORI Preparation. A successful EORI relies on a number of factors. Among them are having knowledgeable personnel, adequate equipment and supply stock, strong customer orientation, and effective training (in an EORI environment, there may be little to no opportunity for one-on-one training to take place; accomplish as much training as possible **prior** to this situation.)

9.3.6.1. Prior to an EORI, review your manning. Using your Unit Manning Document and Air Force Wide/Availability Tasking Summary, ask: "Do I have enough trained personnel to support 24-hour operations at home and deployed locations?" If you do not know what your wartime tasking is, ask your LG people to review and explain your DOC statement. If you do not have the personnel you need, identify the problem to your commander and HQ AMC/IN.

9.3.6.2. Equipment is another critical element. It is your responsibility to ensure you have the materials and tools you need to do your job. Defining what you need and getting it is an on-going battle. In addition to your home station equipment, you need to be familiar with your wartime UTC requirements. If you have equipment shortfalls, document them and make them visible to your commander and HQ AMC/IN.

9.3.6.3. Training is the key to the effectiveness of your personnel and equipment.

9.3.6.3.1. Review your training and ensure it focuses on practical wartime skills (i.e., Crisis Action Team briefings, air-land/airdrop briefings, pre-mission briefings, pre-deployment

briefings, requests for imagery/information, deployed location operations.) Consider what your customers need to do their job and ensure your office trains to provide the best timely, tailored, focused intelligence. These functions should be the first priority of your internal training.

9.3.6.3.2. Local exercises provide additional training opportunities. For these to be effective, your intelligence unit must provide a scenario to drive the exercise, ensure it exercises the unit DOC statement, and requires all unit personnel to exercise wartime skills. We cannot overstate the importance of these exercises as an opportunity to integrate intelligence operations/training with the roles and missions of your commander, crews and support personnel. This is an opportunity to hone your wartime skills, train your commanders and crews on what intelligence can do for them, and identify your problems.

9.3.6.3.3. Establish checklists for all basic products and processes (i.e., briefing/debriefing, change-over, pre-deployment, deployed location set-up/operations, etc.) Train with and use these checklists.

9.3.6.3.4. Participation in other units' exercises, EORIs, and/or major exercises is another good opportunity to build your readiness. Communications with other units, your local plans staff, and HHQ is the first step in taking advantage of these opportunities.

9.3.6.3.5. For airdrop units, take full advantage of your local JA/ATT missions as an opportunity to practice your integration with mission planners, tactics, and aircrews.

9.3.6.4. Build canned briefing packages and fill in the essential information as it comes in. This saves time and enables the SIO to maintain a degree of quality control and consistency in what briefers report to the crews, staff and deploying personnel.

9.3.6.5. Review past ORI and any current EORI reports. Call other units, your NAF, HQ AMC/INX or IGPO. All reports are available through AMC's homepage at **https://amc.scott.af.mil/ig/html/EORIREPO.htm**.

9.3.6.6. Know your unit's mission and plan to support it. You may or may not mobilize and/or integrate augmentees. These requirements vary significantly throughout AMC. The EORI is based on your DOC statement.

9.3.6.7. Establish and maintain a comprehensive situation display. This display should emphasize the enemy Integrated Air Defense System (IADS), friendly operating locations, established air routes, incidents of fighting/attack, and all identified threats to friendly air operations. The situation display is an essential information management tool and should provide the current base-line "snapshot of the war" upon which you base all briefings. The display must contain a legend defining all symbols on your board.

9.3.6.8. Build message shells for RFIs, OSTREP, Imagery Requests, MISREPs, etc. Have these readily available and train people to use them.

9.3.6.9. Establish procedures to monitor unit tasking, briefing and debriefing requirements. Ensure all personnel know how to read and follow these procedures, whether on a dry-erase board, computer spreadsheet, or handwritten chart.

9.3.6.10. Establish a combined Operations and Intelligence briefing/debriefing team. Educate your customer on the what, why and how of your wartime function. A clear understanding of

responsibilities is important to ensure a coordinated, tailored response to your organization's mission. Intelligence will manage information of the overall situation and threats to operations. Areas of shared responsibility might include the management of SPINS, communications and safe passage procedures, medical intelligence, operationally significant debrief information, and the preparation, issue, and return of classified mission support packages. Continuously solicit feedback from your customers to validate your products and processes.

9.3.7. Inspector/Unit Interaction. This area allows face-to-face contact between unit personnel and functional experts. This interaction is designed to create an environment where you and the inspector can discuss your organization and/or program status. It also gives you the opportunity to voice problems that you were unable to solve through your chain of command. These problems normally relate to areas that lower levels cannot correct such as inadequate facilities, restrictions to training programs, insufficient manning, or over-tasking. Inspections are your chance to show the world how effective you are, and also to put experienced staffs to work for you. In addition, person-to-person contacts permit inspectors to provide insight that can benefit you. After reviewing numerous units and programs, inspectors can offer sound techniques and procedures and suggest effective methods to make your unit and the Air Force more efficient.

9.3.8. Preparation Pointers

9.3.8.1. Be Prepared. Prepare for an inspection by ensuring your work area is clean, neat, and orderly. You should make your work environment as pleasant as possible. Also, ensure you and the people you supervise are complying with dress and appearance standards. The little things may not appear in the final report, but they may affect the way the inspector writes the report.

9.3.8.2. Be Positive. Show a positive, "can do" attitude. Talk about the good points of your functional area. Feel free to discuss major problems with the inspector that may need out-of-house attention, but avoid letting your "problems" outweigh your attributes.

9.3.8.3. Document Unit Actions. Document in written format any/and all actions that impact your organization’s ability to perform its mission. Everything from training to mobility issues to requests from higher headquarters should be documented; not just for your purpose, but potentially for IG evaluation purposes.

9.3.9. Inspection Checklists

9.3.9.1. The checklists on the following pages are not intended to replace checklists located in other sections of this handbook or other AF or command directions or instructions. Their purpose is to augment the inspector in evaluating your unit’s mission effectiveness. Apply the checklists to your unit’s operational mission.

9.3.9.2. Checklists that your unit will be evaluated on can be located throughout this handbook and AMCP 90-202, *Operational Readiness Inspection Guide*. Additionally, AMCI 90-201, *The Inspection System*, defines the command’s IG program, its objectives, and other supplementary information.

9.3.9.3. The IG’s goal in evaluating your unit is to do so in a non-threatening manner and is not intended to impede the way you do your job. Questions will be asked and proof of accomplishment (documentation) may be requested. Unit preparation is the key to your unit and your personnel standing out among all the others!

CHECKLIST		PAGE 1 OF 9 PAGES		
TITLE/SUBJECT/ACTIVITY **AMC CONTINGENCY/WARTIME/EORI CHECKLIST**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
NOTE: Use visual aids for all elements in the intelligence portion of these briefings. 1. Does the unit have and use locally tailored operating instructions/checklists for the following areas? A. Initial Actions. B. Battle Staff (BS)/Crisis Action Team (CAT) briefing support. C. Single Integrated Operational Plan (SIOP) Briefing/Assmpt of Alert Briefing. D. Requests For Information (RFI). E. Requests For Imagery (RI). F. Requests for Geospatial Information and Services (GI&S). G. Support to deployment mission planning. H. Intelligence personnel and equipment for deployment operations and/or home station support. I. Significant events board or log. J. Updating situation displays and/or Orders of Battle (OB). K. Support to pre-deployment briefings for aircrews. L. Support to pre-deployment briefings for non-aircrew personnel. M. Set-up operations at the FOB/FOL. N. Pre-mission/employment briefings. O. Shift changeover briefing. P. Debriefing. Q. Reporting to include: (1) Status at FOB/FOL. (2) Mission Reports (MISREP).				

CHECKLIST		PAGE 2 OF 9 PAGES		
TITLE/SUBJECT/ACTIVITY **AMC CONTINGENCY/WARTIME/EORI CHECKLIST**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
	(3) Intelligence Report (INTREP). (4) Intelligence Summary (INTSUM). (5) On-Station and Off-Station Reporting (OSTREP). (6) Downed aircrew. R. Redeployment actions. S. Emergency actions. 2. Does the unit maintain an intelligence database? A. Is the data periodically reviewed for currency? B. Does the unit conduct analysis of the data in the database? C. Does the unit tailor the data to meet mission needs? D. Are situation displays and/or OB boards posted with applicable threat data? E. Does the unit identify gaps in the database? Do they establish the following: (1) Requests for Information (RFI). (2) Requests for Imagery (RI). (3) Requests for Geospatial Information and Services (GI&S) Products. F. Does the unit follow-up above requests? 3. Does the unit coordinate/pass critical mission impacting information to other base agencies? If applicable, are the following agencies contacted? A. AFOSI. B. Security Forces. C. Tactics/Current Ops/Plans Branch. D. Threat Working Group.			

CHECKLIST		PAGE 3 OF 9 PAGES		
TITLE/SUBJECT/ACTIVITY **AMC CONTINGENCY/WARTIME/EORI CHECKLIST**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
	E. Medical. F. Readiness (Formerly Disaster Preparedness). G. Does the unit provide timely updates to the above agencies? 4. Does the unit prepare and present briefings to the Battle Staff (BS) and or Crisis Action Team (CAT)? Do briefings cover the following: A. Security classification (at the beginning and end). B. "Current as of" time. C. Significant military/political events. D. Threat to home station. E. Threat to FOB/FOL (if applicable). F. Brief overview of the Orders of Battle. G. Friendly operations in theater which impact/support unit operations. H. Probable courses of enemy action. I. OPSEC/COMSEC reminders. 5. Are specialized briefings prepared and presented to base agencies/personnel as required? 6. Are briefings tailored to meet mission requirements? 7. Has the unit coordinated with the Individual Mobility Officer (IMO) to assist in the development of a Schedule of Events (SOE)? 8. Does the unit comply with the SOE? 9. Does the unit prepare and present tailored pre-deployment briefings for deploying non-aircrew personnel? Are these briefings specific to each FOB/FOL and do they contain the following information: A. Security classification (beginning and end). B. "Current as of" time.			

CHECKLIST		PAGE 4 OF 9 PAGES		
TITLE/SUBJECT/ACTIVITY **AMC CONTINGENCY/WARTIME/EORI CHECKLIST**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
	C. Reason for deployment. D. General situation. E. OB in the deployment area. F. Friendly situation and forces in the deployment area. G. Threat in theater. H. Threat in FOB area. I. OPSEC/COMSEC reminder. 10. Does the chief of intelligence direct and control his/her personnel including: A. Are personnel managed effectively to accomplish critical actions? B. Are shortfalls in required manning identified and reported to HHQ? C. Does the unit integrate additive forces (Reserve and IMA) into the mission (as applicable)? (1) Does the unit prepare for these personnel in advance to ensure: (a) Training on wartime tasks to facilitate a smooth transition into the mission? (b) Identification and procurement of equipment for gained personnel? (2) Are personnel effectively integrated into the mission? D. Has the unit smoothly and safely transitioned to 24 hour operations? 11. Has all pertinent incoming intelligence been analyzed for impact on deployment operations? 12. Does the unit post situation displays with OB and applicable threat data? 13. Does the unit tailor all pertinent incoming intelligence information to meet mission requirements? 14. Does the unit provide route threat assessment to applicable mission planning?			

CHECKLIST		PAGE 5 OF 9 PAGES		
TITLE/SUBJECT/ACTIVITY **AMC CONTINGENCY/WARTIME/EORI CHECKLIST**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
15. Does the unit coordinate and assist aircrews and combat survival personnel in the preparation of evasion plans of action (if applicable)?				
16. Does the unit provide tailored, route specific pre-deployment briefings to aircrews? If necessary, do the briefings cover the following information: A. Security classification (beginning and end). B. "Current as of" time. C. Reason for deployment/mission. D. General situation/OB in the deployment area. - Ground - Air - Naval E. Friendly situation and forces in the deployment area. F. Possible en route threats - route specific - leg by leg - from takeoff to landing. (Don't forget often overlooked issues such as: local situation, EW/GCI, concerns regarding other friendly forces.) G. Alternate/emergency airfields. H. Air Force Spectrum Interference Resolution (AFSIR) - formerly MIJI. I. SAR and SERE information. J. OPSEC/COMSEC reminder. K. Sanitization reminder. L. EEIs (HHQ or theater developed). M. ISOPREP Review reminder. N. Debriefing instructions.				
17. Has the unit established contact with theater HHQ Intelligence? Does contact continue?				
18. Has the unit run their FOB set-up checklist?				

CHECKLIST		PAGE 6 OF 9 PAGES		
TITLE/SUBJECT/ACTIVITY **AMC CONTINGENCY/WARTIME/EORI CHECKLIST**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
19. Has the unit informed the local comm center of their arrival and have they submitted a letter authorizing personnel for message pick-up?				
20. Has the unit submitted an On Station Report (OSTREP) to HHQ (AMC/INF, Parent NAF, gaining theater intelligence)? Does the report include:				
	A. Current manning level.			
	B. Additional manning required.			
	C. Communications abilities to include fax, phone, and STU-III capabilities.			
	D. Approximate workload.			
	E. Shift schedule.			
	F. Other information deemed necessary (Ref AMCI 14-102).			
21. Does the unit continue to analyze all incoming information for mission impact?				
22. Are threats to the FOB/FOL and unit tasking posted to displays/OB boards?				
23. Is information tailored/prioritized to meet mission requirements?				
24. Are threats impacting FOB/FOL briefed to the GOC/WOC and passed to the FOL?				
25. Are members of the threat working group included in the threat discussions?				
26. Does the unit prepare and present briefings to the Battle Staff (BS) and/or GOC/WOC/Threat Working Group? Are the briefings tailored and timely, and do they cover:				
	A. Security classification (beginning and end).			
	B. "Current as of" time.			
	C. Significant military/political events.			
	D. Threat to home station (if applicable).			
	E. Threat to the FOB/FOL.			
	F. Brief overview of the Orders of Battle.			

CHECKLIST		PAGE 7 OF 9 PAGES		
TITLE/SUBJECT/ACTIVITY **AMC CONTINGENCY/WARTIME/EORI CHECKLIST**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
	G. Friendly operations in theater which impact/support unit operations. H. Probable courses of enemy action. I. OPSEC/COMSEC reminders. 27. Does the unit coordinate and assist aircrews and combat survival personnel in the preparation of EPAs? 28. Does the unit provide tailored route threat assessment to the Mission Planning Cell? 29. Does the unit provide combat mission folder (CMF) inputs (EWO only)? Do these inputs cover the requirements in local CMF checklist? 30. Does the unit provide route threat assessment to mission planning? 31. Does the unit provide tailored route specific pre-mission/employment briefings to aircrews? Do the briefings cover: A. Security classification (beginning and end). B. "Current as of" time. C. Reason for mission. D. General situation/OB in the deployment area. - Ground - Air - Naval - MOB - EOB E. Friendly situation and forces in the deployment area. F. Possible en route threats - route specific - leg by leg - from takeoff to landing. (Don't forget issues such as: local situation, EW/GCI, concerns regarding other friendly forces.) G. Immediate target/operating area (DZ, LZ, EZ, AR Track) threats. (Often better if incorporated into the en-route threats portion.) H. Alternate/emergency airfields. I. AFSIR.			

CHECKLIST		PAGE 8 OF 9 PAGES		
TITLE/SUBJECT/ACTIVITY **AMC CONTINGENCY/WARTIME/EORI CHECKLIST**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
	J. SAR and SERE information. K. OPSEC/COMSEC reminder. L. Sanitization reminder. M. EEIs (HHQ or theater developed). N. ISOPREP reminder. O. EPA Review Reminder. P. Debriefing instructions. 32. Does the unit prepare, issue, and inventory Personnel Recovery Kits (PRKs) to aircrews? Does the kit contain: A. Evasion chart of mission area. B. Pointee-Talkee. C. Blood Chit (if required). D. Other materials as deemed necessary by SERE specialists and intelligence personnel 33. Does the unit provide material for inclusion in the mission folder (if applicable)? 34. Do AWADS/SOLL units provide the following material for inclusion in the mission folder? A. RECCEXREP (if provided, N/A for AFRC). B. Terrain analysis. 35. Does the unit contact HHQ with requests for information, imagery, and GI&S products as required? Is follow-up accomplished? 36. Is OPSEC/COMSEC enforced? 37. Does the unit react properly to threat condition changes (FPCON) and attack warnings? Do reactions to warning signals include the following: A. Taking cover. B. Donning equipment. C. Use of antidotes.			

CHECKLIST		PAGE 9 OF 9 PAGES		
TITLE/SUBJECT/ACTIVITY **AMC CONTINGENCY/WARTIME/EORI CHECKLIST**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
	D. Decontamination procedures.			
	E. First aid and buddy care.			
38.	Does the unit suspend non-critical tasks when appropriate?			
39.	Does the unit continue mission essential tasks?			
40.	Are tasks prioritized and accomplished in an effective manner?			
41.	Does the unit use secure communications to advise subordinate units and theater HHQ of critical developments impacting the units?			
42.	Does the unit follow-up with timely Intelligence Reports (INTREPs)?			
43.	Does the unit have a mission tracking system to ensure aircrews receive timely debriefings? Is the system effective?			
44.	Is every mission debriefed by intelligence?			
45.	Are Mission Reports (MISREPs) submitted IAW AMCI 14-102 or theater requirements in a timely manner and in the correct format?			
46.	Is critical data from MISREPs included in aircrew briefings?			
47.	Is critical data from MISREPs passed to HHQ, theater assets, and subordinate units?			

9.4. Staff Assistance Visits (SAV). An AMC Intelligence Unit SAV is highly focused on the core processes employed by a unit during all phases of operations. While IG inspections seek to evaluate a unit's operational capability, a SAV seeks to evaluate the administrative and management functions that form the foundation from which the intelligence flight operates.

9.4.1. AMC/INXU endeavors to conduct SAVs on all active duty units on a biannual basis. The overall goal of the unit SAV program is ensure all AMC intelligence units are prepared to efficiently carry out their assigned missions. To achieve this goal, unit SAVs strive to meet four distinct objectives: to

ensure unit compliance with applicable Air Force and AMC instructions and identify areas for improvement; to provide detailed recommendations to correct identified deficiencies; to identify opportunities for HQ AMC/IN to improve support to the units; and finally, to provide detailed, written feedback to the OSS/IN, OSS/CC, and AMC/IN.

9.4.2. AMC/INXU will publish a tentative SAV schedule at the beginning of each fiscal year outlining the anticipated SAV times for each of the active duty units over the next two years. Specific times will be coordinated through AMC/INXU and the unit IN before proceeding through the normal AMC Gatekeeper procedures, outlined in HOI 36-2803, *Support for Higher Headquarters Gatekeeper Program*, which can be found at **https://public.scott.af.mil/hqamc/pubs/hqoi.htm**.

9.4.3. The AMC/IN Unit Self-Assessment Checklist is primary document used to conduct a SAV. It should also be the primary document used by the unit in conducting their own semi-annual self-inspections. The checklist can be found on the AMC/IN's unclassified homepage under Unit Readiness, Unit Self-Assessment Checklist, or by going directly to **https://140.175.125.145**, and select "Reference". This checklist provides an excellent gauge for determining weak areas in unit operations.

9.4.4. A typical SAV may last from two to five days. The SAV team members first provide an in-brief to the OSS/CC or their representative. Next, team members require the unit IN to provide a general unit briefing outlining the flight's internal organization, members, major accomplishments over the prior year, and the main priorities for the unit. The SAV team will then begin taking an in-depth look at your unit's core processes. It is a quick, but extensive, process that will require hours of discussion with all flight members, especially those in charge of major programs. However, it shouldn't be an intimidating process. There is no evaluation or grading in a SAV. The whole purpose is to identify and correct problem areas before they generate mission impact.

9.4.5. Final SAV reports are coordinated through the HQ AMC/IN staff, and are then provided to the OSS/CC and OSS/IN. The SAV report provides a detailed description of team observations on all programs/issues discussed at the unit. It also provides recommendations for corrective actions to be taken by the OSS and the HQ AMC/IN staff in order to correct observed deficiencies.

Chapter 10

PERSONNEL RECOVERY PROGRAM

10.1. General. Personnel Recovery (PR) is the umbrella term for operations focused on recovering captured, missing, or isolated personnel. It is the sum of military, civil, and political efforts to obtain the release or recovery of personnel from uncertain or hostile environments and denied areas. This includes U.S., allied, coalition, friendly military, paramilitary forces, and/or others designated by the President of the United States or the Secretary of Defense. PR includes, but is not limited to: theater Search and Rescue (SAR); CSAR; Survival, Evasion, Resistance and Escape (SERE); E&R; and coordinated/negotiated, as well as, forcible recovery options. PR may occur through military action, action by non-governmental organizations, U.S. Government-approved action, diplomatic initiatives, or any combination of these options (DoD Directive 2310.2, *Personnel Recovery*.)

10.2. Historical Background.

10.2.1. World War II (WW II). During WW II, incomplete and fragmentary records were kept on successful E&R episodes of the three major theaters (Asia, Europe, and North Africa.) At the end of WW II, there were 110,000 living ex-Prisoners of War (POWs) and well over 45,000 successful U.S. evaders. Few, if any, of these combat survivors had received any combat survival training.

10.2.1.1. Asia. In Asia, the total number of U.S. POWs taken by Japan was approximately 25,000. Almost 8,500 of these (34 percent) died of neglect or abuse prior to liberation. Evader statistics are very sketchy for this theater. We do know that over 1,000 U.S. evaders were assisted in China, 574(+) in Burma, 1,000(+) on New Guinea and the Solomon Islands, and 648 in French Indo-China from April to June, 1945, for a total of 3,222 assisted evasions during that 3-month period. No official statistics have been found for successful evasions in the Philippines, Borneo, or the numerous islands throughout the Pacific, but there are many individual stories.

10.2.1.2. Europe. Much more information was found on POWs and evaders in Europe, but the figures have not been broken down by branch of service. At the end of the war, 93,600 Americans were prisoners of the Germans. Most of these were aircrew personnel who had been shot down during bombing missions over France and Germany. The number of successful evaders in Europe stood at more than 41,246; 6,000 of which were returned by submarine, clandestine boat, or aircraft prior to D-Day. In the 5 months following D-Day, over 1,393 evaders or escapees (flyers) walked back to friendly lines (527 shot down before D-Day, 666 after D-Day, and over 200 were early escapees.) Neutral Switzerland turned over 1,503 U.S. personnel (790 flyers) by December 1944. Of these 41,000(+) successful evasions, approximately 38,000 were accomplished with some form of civilian assistance; nevertheless, nearly all Americans had to evade unassisted for some time to stay free until they linked up with either civilians or partisans.

10.2.1.3. North Africa. The least amount of information was found on North Africa. It appears an unknown number of POWs were shipped back to Europe from North Africa, but members of 382 aircrews were able to evade successfully back to their own lines. Even though the longest episode took 29 days and covered 350 miles, the average was only 5 days and 50 miles. Out of the 382 aircrews (crew size 1-10), 142 individuals died from environmental causes after reaching the ground safely.

10.2.2. Korean War. By the beginning of the Korean War, the U.S. Air Force had begun to provide its forces in Strategic Air Command (SAC) with survival training. The training emphasis was primarily to survive and evade to a recovery site or border, and resist enemy exploitation in the event of a conflict with the Soviets. Many, but not all, aircrew members had evasion training when they were sent to the Korean Theater. Statistics for this war were more complete than during WW II. During the Korean War, 1,690 Air Force personnel were downed in enemy held territory. Two hundred forty eight POWs were returned in 1953. Helicopters and amphibious aircraft were dedicated to aircrew recovery and managed to recover 175 U.S. and 86 Allied (United Nations (U.N.)) flyers shortly after being downed. There were a total of 273 successful returns of U.S. flyers. Ninety-five of those American flyers were able to evade on foot to friendly lines and three others escaped and returned to friendly forces without assistance. The longest episode lasted 83 days.

10.2.3. Post-Korean War Guidance.

10.2.3.1. After analyzing the combat survival experiences of the Korean and previous wars, President Eisenhower signed Executive Order 10631 creating the Code of Conduct (CoC) as a moral guide to behavior for U.S. military personnel facing evasion or captivity. In 1955, the Secretary of Defense issued training requirements and guidelines to the services regarding implementation of this order. They include, in part:

10.2.3.1.1. "Specialized training appropriate to service and individual requirements must be given in evasion, escape, resistance, prisoner organization and survival."

10.2.3.1.2. "These programs should be progressive from General to specialized training and continue throughout the career of the service member."

10.2.3.1.3. "This training would be conducted within normal training systems, special courses of instruction and by realistic field exercises and maneuvers."

10.2.3.2. The Air Force decided that almost all its flying personnel should receive this training to prepare them for numerous global contingencies. The SAC Survival School transferred to Air Training Command and unit-level survival continuation training became a requirement throughout the Air Force.

10.2.4. Southeast Asia (SEA). The Air Force lost 1,678 fixed wing and 59 rotary wing aircraft in SEA between 1963 and 1973.

10.2.4.1. Evaders in SEA owed a large part of their success to air recovery efforts developed to retrieve them. Air recovery efforts were a major factor in successful evasion. However, almost all personnel who were recovered had to utilize evasion training. Evaders had to take evasive action on the ground to avoid the enemy long enough for recovery assets to arrive in the general area and for the evader to guide them to his hiding place. The "walk-back" option was not practical due to the distances and jungle or mountainous terrain. However, air superiority allowed helicopters from all Services to be consistently within radio range. The frontlines/friendly forces were defined by where aircraft could successfully conduct rescue operations. The technology of helicopters and radios, together with effective utilization of helicopters in the mission planning cycle, allowed about 75 percent of SEA evaders to be recovered within 6 hours of being downed.

10.2.4.2. Three hundred thirty three USAF personnel from these downed aircraft survived as POWs and were returned at the end of the conflict. Another 1,201 USAF personnel successfully evaded until USAF air recovery assets recovered them. USAF recovery helicopters picked up a

total of 3,883 people in distress in SEA (the previously mentioned USAF people plus 926 Army, 680 Navy, 555 allied military, 476 civilians, and 45 unidentified personnel.)

10.2.4.3. Army, Navy, Marine, and Air America assets recovered other USAF evaders, but the exact numbers are unknown. Seventy-five to 86 percent of all recovery operations were conducted while under fire. The longest successful USAF evasion episode in North Vietnam lasted 23 days.

10.2.5. Impact of Evasion Training. Even though we know the numbers of successful evaders are incomplete, tallying and comparing the percentages of POWs and evaders produces interesting results. It appears that flyers with no evasion training downed in WW II, in an area with basically friendly civilians, who for the most part were similar in appearance, had only a 30 percent success rate as evaders. In the Korean War, aircrews with some evasion training and no sympathetic or similar looking population experienced a 52 percent success rate as evaders. In SEA, almost all USAF aircrews had evasion training, and with a hostile, dissimilar population, they still had a success rate as evaders of over 78 percent.

10.2.6. Desert Storm/Southwest Asia (SWA). Despite all the advances made up through the end of the Vietnam Conflict, Desert Storm evasion and recovery cases revealed serious lapses in pre-crisis preparation. The following paragraphs discuss key points and trends revealed through extensive after-action analysis of such events. They provide a harrowing tale of the conditions our downed aircrews were operating under during this conflict.

10.2.6.1. Premission Preparation.

10.2.6.1.1. In certain cases, DESERT STORM aircrews lacked one of the most important factors for successful evasion - preparation. Aircrew members must make evasion planning an integral part of detailed mission preparation. Failure to accomplish this may result in a more problematic scenario and complex recovery process. SERE Mobile Training Teams (MTT) deployed to provide refresher training to individuals subject to isolation in hostile territory. However, there was a general failure to maximize this training: two evaders did not attend a MTT session even though they were available. Most evaders were unfamiliar with the use of their survival equipment.

10.2.6.1.2. Unfamiliarity with the published CSAR SPINs and individual survival equipment was evident in most scenarios.

10.2.6.1.3. Last minute changes in mission profiles resulted in some evaders failing to complete an Evasion Plan of Action (EPA).

10.2.6.1.4. Following repatriation from captivity, several unsuccessful evaders recommended Premission briefings to include information on non-radio contact procedures. Those individuals believed the lack of a survival radio and there inability to contact recovery forces were key factors in their unsuccessful evasion.

10.2.6.1.5. Some evaders failed to fully hydrate themselves before departing on missions into the desert environment. Being dehydrated with a limited reserve of water caused some evaders to quickly deplete available water supplies and forced them to increase the risk of capture by searching for water.

10.2.6.1.6. Securing all loose items prior to departure is an acceptable practice within the aviation community. This practice also applies to ensuring all evasion items are properly secured to the survival vest or in the flight suit. High-speed ejection can (and did) force open partially

closed G-suit and flight suit pockets, scattering improperly stored survival, weapon, and communication gear.

10.2.6.2. Pre-egress Actions. Most evaders did not have time to make emergency calls prior to ejection.

10.2.6.3. Egress Injuries. The injuries sustained during ejection ranged from minor bumps and bruises to twisted knees and broken bones. One evader believed his two broken arms and a dislocated shoulder limited his ability to evade. Another evader, recovered by ground forces, had several broken bones and a broken jaw that impacted evasion. An evader who flew without gloves suffered burns to his hands before and during egress. His burned hands were rubbed raw when he dug a small hole for concealment using his survival knife. In his post-recovery debrief, he specifically mentioned that he regretted not wearing gloves to protect his hands.

10.2.6.4. Parachute Descent Actions. On two separate occasions, evaders elected to use their survival radios during the parachute descent. One evader believed he received an acknowledgment from Airborne Warning and Control System (AWACS); however, he failed to follow-up this acknowledgement. He feared losing his radio since it was not secured to his vest. Once on the ground, he contacted his wingman, who then contacted AWACS.

10.2.6.5. Initial Post-landing Actions. Quick movement away from landing sites was of primary concern to evaders. Many downed flyers did not have the opportunity to evade due to the proximity of enemy forces. In a few cases where individuals were able to evade, their sense of urgency to move away from landing sites caused some of them to make mistakes. Initial post-ejection shock was a factor in some of the decisions made and actions taken.

10.2.6.6. Communications. Many evaders were concerned about establishing radio communication with AWACS, their wingman, or other coalition aircraft. Evaders experienced various degrees of difficulty in operating their survival radios. Failure to turn off emergency beacons, which overrode their radio/voice transmissions, also created problems for evaders.

10.2.6.7. Movement. Movement in hostile, unfamiliar terrain can be risky. If an evader is uncertain of the surrounding terrain, location of enemy forces, or unaccustomed to evasion tactics and techniques, the results are usually disastrous.

10.2.6.8. Recovery. Whenever an individual is recovered with the assistance of a dedicated recovery force, the most critical aspect of that recovery is the moment when the evader and the recovery force come together. The moment of contact is very tense because it requires two parties, unknown to each other and in hostile territory, to meet without being detected by either enemy forces or elements of the local population and without compromising either party's security. This moment of contact requires a great deal of planning.

10.2.7. General Historical Conclusions.

10.2.7.1. During WW II, our high-risk personnel went to war with little or no combat survival training. Some of them took it upon themselves to study previous World War I escape stories in an attempt to prepare for evasion or captivity. Many, however, did not. Before and during the Korean War, the U.S. military had learned from the shortcomings of WW II and began training high-risk personnel to deal with combat survival. It appears to have paid off with a much higher percentage of evaders staying free until recovered or until they could walk back.

10.2.7.2. After the Korean War, training of high-risk personnel was modified again. Training in the employment of recovery devices was added, along with signaling and communicating with recovery assets; survivor directed air strikes; radio discipline; evasion movement and concealment; and a theater specific school was created, all to adjust to the needs of our combat survivors--and it apparently worked.

10.2.7.3. Combat Search and Rescue came to full maturity during the Vietnam conflict. The leaps in technology following WW II and Korea created an entirely new set of difficulties for evading personnel and recovery forces. Technological and tactical employment advances also greatly aided evaders and their rescuers. Developed in Korea and perfected in Vietnam, recovery force tactics evolved into a highly integrated fixed and rotary wing operation. When needed, substantial amounts of firepower could be rapidly concentrated into an integrated recovery force.

10.2.7.4. The DESERT STORM evasion experience clearly identified the value of continuing evasion training and the MTT concept. Unfortunately, some aircrews had to endure captivity because they and the forces that supported them failed to utilize the available training. Intelligence professionals must provide their aircrews the best threat, force, and population disposition information possible.

10.2.7.5. It is once again time to learn from the past and prepare to meet the needs of the future by maintaining and improving the evasion training programs that have evolved through experiences over the past 50 years. Potential enemies have made technological advances in the area of lightweight, inexpensive, anti-aircraft missiles and quick, accurate radio direction finding (DF) equipment. Evasion and recovery strategies for U.S. military personnel need to include enhanced evasion training. It is absolutely essential that potential evaders receive training that will enable them to evade and remain free, find water and food, protect themselves from the environment, and accurately navigate to recovery sites away from the enemy threat for recovery by conventional or unconventional means.

10.2.7.6. The confidence and knowledge provided by evasion training might also benefit those unfortunate evaders who are not successful. Even when successful evasion appears impossible, a wholehearted attempt may be very valuable to a POW's resistance. Every day spent evading can make the POW a poorer target for exploitation. During an interrogation for perishable, tactical information, the adverse effects of evasion may be beneficial. Answers of "I don't know," or "I can't remember" may seem more plausible, and may be accurate when the prisoner's appearance and aroma indicate he's been evading for a week or two.

10.3. The USAF Survival, Evasion, Resistance, and Escape (SERE) Program. The Air Force SERE program is a critical component of the overarching DoD Personnel Recovery Program. It encompasses SERE Code of Conduct Training (CoCT), SERE Code of Conduct Continuation Training (CoCCT), and PR operational support required to enable war fighters to return to friendly control after isolation due to enemy actions, aircraft emergency, or other unforeseen events. The SERE program is designed to ensure war fighters receive the appropriate type and level of SERE training and PR preparation throughout their career. It also establishes and formalizes critical links in the flow of information, and implements SERE and PR Joint Tactics, Techniques and Procedures (JTTP) permitting integration with other war fighting functions and with the war fighter's other missions. Information on SERE programs can be found at **http://www.jpra.jfcom.smil.mil** under "Products and Information."

10.3.1. Code of Conduct Training (CoCT). The SERE program is grounded in the CoC. The CoC is the foundation underpinning the war fighter's PR preparation and training. The Code serves as a moral and ethical guide for behavior (legislatively backstopped by the Uniform Code of Military Justice (UCMJ)) for isolated DoD operators including evaders, POW, peacetime governmental detainees, and hostages. Training war fighters on their obligations under the Code of Conduct is critical to reducing the military and political impact of isolated war fighters. Effective CoCT improves operator confidence and morale, and provides decision-makers a high degree of confidence that isolated operators will maintain honor, protect sensitive operations and information, and actively resist the enemy's attempts at exploitation. There are three levels of CoCT:

10.3.1.1. Level A is the minimum level of understanding for all members of the Armed Forces, attained by all personnel during entry-level training. It educates new accessions on the CoC articles and their responsibilities to uphold the code. Level A is revisited during PME courses.

10.3.1.2. Level B is the minimum level of understanding needed by personnel who have a moderate risk of capture during peacetime or combat. This training is intensive and covers all elements of combat survival training. With the CoC at its core, level B instruction teaches potential detainees techniques to employ in resisting enemy attempts to exploit them and to continue efforts to resist and/or escape. Level B training can only be conducted by fully certified SERE Specialists.

10.3.1.3. Level C training is the minimum level of understanding needed by personnel who have a high risk of capture or are vulnerable to greater-than-average exploitation by a captor during peacetime or combat. Level C includes senior Air Force officials assigned to or visiting high threat areas. This training is basically the same as level B with additional "hands-on" resistance training. Level C training may only be conducted by certified SERE Specialists and is conducted in a strictly controlled environment.

10.3.2. Code of Conduct Continuation Training (CoCCT). CoCT must continue throughout the career of affected personnel. SERE CoCCT is a combination of refresher SERE CoCT and additional theater-specific Contingency SERE Indoctrination (CSI) training. CoCCT is designed to help personnel maintain critical SERE skills gained at initial formal SERE CoCT schools and to tailor SERE skills for specific missions/platforms and deployment locations. Conduct-After-Capture CoCCT, commonly referred to as Resistance Training (RT), provides refresher training for wartime, peacetime detention, and hostage/terrorist captivity situations. Only qualified SERE Specialists, AFSC 1T0X1, will conduct RT refresher training. Hands-on, Level C-like caliber role-play instruction is specifically prohibited without HQ USAF/XOO approval and validation. Intelligence personnel are not qualified to conduct this type of training and will not, under any circumstances, attempt to do so.

10.4. Personnel Recovery Operational Support Program. The PR Operational Support Program is a joint effort of unit-assigned SERE Specialists, Life Support, and Intelligence personnel. The intent of the program is to manage and maintain those PR programs and products that enhance the survivability of personnel who may become isolated from friendly forces. The program includes: ISOPREP maintenance and training; EPA development, maintenance, and training; PR Kit development, maintenance, and training; Pre-deployment training on theater PR programs, requirements, and procedures. Support information for unit support programs is available at **http://www.jpra.jfcom.smil.mil/products**. Unit Intelligence plays a critical role in every aspect of this program.

10.4.1. DD Form 1833, Isolated Personnel Report (ISOPREP). The ISOPREP is the single most critical document to facilitate combat recovery of isolated personnel. Recovery forces attempting to res-

cue isolated personnel are extremely vulnerable during the actual recovery phase. During the Vietnam conflict, the adversary often used a downed aircrew member as bait to draw recovery forces into an ambush. There have been repeated incidents of the adversary attempting to "spoof" a recovery force into an area of the enemy's choosing to allow such an ambush. The Joint Tactics, Techniques, and Procedures (JTTP) for CSAR (Joint Pub 3-50.21) warns, "…isolated personnel will not normally be recovered until there identity has been verified." Recovery forces use the data contained on the ISOPREP to establish this positive identification prior to "going in" for the pick-up.

10.4.1.1. Direction and guidance concerning ISOPREP generation and maintenance can be extracted from the pubs referenced at the end of this chapter. However, most of that direction and guidance comes in the form of joint-level doctrine. The Joint Personnel Recovery Agency (JPRA) has issued definitive "in a nutshell" guidance in the form of a message (131800Z NOV 2000, SUBJ: ISOPREP PROGRAM) to fill the void between joint doctrine and operational direction. This message, and a wealth of other information concerning personnel recovery issues, can be found on the JPRA Intelink-S Homepage at **http://www.jpra.jfcom.smil.mil/**.

10.4.1.2. We currently have two ISOPREP formats: the DD Form 1833, *Isolated Personnel Report*, and the Digital ISOPREP. The first one, DD Form 1833, is printed on durable 8.5 X 11 inch card stock, and contains identification and authentication data. This form is available in form flow for printing and viewing. The second is a computer based soft copy of the DD Form 1833. (**NOTE: The creation of a Digital ISOPREP does NOT do away with the requirement to maintain two cardstock copies of DD Form 1833**.) The following paragraphs detail specific requirements when filling out DD Form 1833, after which an example is provided.

10.4.1.2.1. ISOPREP Generation. The ISOPREP becomes a permanent record when a member becomes isolated and is a vital part of long term POW/Missing in Action (MIA) accountability. Once completed, the ISOPREP is classified CONFIDENTIAL and will be maintained by the appropriate unit intelligence or operations personnel. Affected personnel complete the ISOPREP upon assignment to their first operational unit and review it at least semi-annually thereafter. During combat operations, personnel must review their ISOPREP prior to the first mission each day, and as often as is deemed necessary thereafter.

10.4.1.2.2. Every effort must be made to ensure that the ISOPREP is completed correctly the first time. Information, such as authentication numbers and statements, developed with unsatisfactory standards should be corrected in a low threat environment such as homestation, NOT in theater where combat sorties are being flown. The reason to wait is to avoid a compromise in the authentication process should an isolated operator revert back to what was first developed under the stress of an actual recovery effort.

10.4.1.2.3. The hardcopy ISOPREP may be typed or hand-written on DD Form 1833. If the ISOPREP is hand-written, the individual must print clearly and legibly.

10.4.1.2.3.1. Blocks 1-13 are self-explanatory.

10.4.1.2.3.2. Block 14, Authenticator Number. This number is written in pencil and must:

10.4.1.2.3.2.1. Not be part of military records or public information.

10.4.1.2.3.2.2. Produce a minimum of four unique answers by adding, subtracting, or multiplying the four digits. The following are examples of good numbers: 8143, 6392, 9463.

10.4.1.2.3.2.3. Be four different numbers with no repeats. Numbers such as 7777, 2799, 3863, etc. are not good choices. The repeated digits are easily compromised if added, subtracted or multiplied.

10.4.1.2.3.2.4. Not be sequential, i.e., 1234, 5678, 6543, etc.

10.4.1.2.3.2.5. Not use the digit zero (0) anywhere in the sequence (i.e., 0179.) This greatly limits the number of authentication possibilities.

10.4.1.2.3.3. Block 15 is self-explanatory.

10.4.1.2.3.4. Blocks 16 - 18 are reserved for Joint Search Rescue Center (JSRC) or Rescue Coordination Center (RCC) personnel.

10.4.1.2.3.5. Block 19 is a spare block. The theater JSRC or equivalent generally determines additional data to be entered in this block. Do not use this block unless directed by such authority.

10.4.1.2.3.6. Blocks 20-23, Personal Authentication Statements. These statements are small declarative paragraphs, not questions and answers. They must be written in pencil and meet the following standards:

10.4.1.2.3.6.1. Statements must be simple, declarative recollections of strong memories based upon real personal events that have occurred to the individual. They must be easily and immediately remembered, even under the most stressful of circumstances.

10.4.1.2.3.6.2. Do not invent stories that may not be remembered during an actual recovery due to the stress of the situation.

10.4.1.2.3.6.3. Do not use statements that may be subject to change. ‘Favorite’ statements are not to be used, because they tend to change over time. Don’t use statements that may be true today, but false in the future. Many people use the same authentication statements for an entire twenty or thirty year career. An example of such a statement would be, "My current dog is a black lab named Batman. He has a white blaze on his chest and a white tip on his tail. His original owners called him Dipstick." While this statement may be factual today, this dog will most likely not be my "current dog" in twenty years.

10.4.1.2.3.6.4. Statements must provide enough detailed facts to allow a minimum of four questions to be derived from each.

10.4.1.2.3.6.5. Avoid the use of slang or jargon that may not be understood by the recovery forces. Simple English works best. If the recovery force cannot understand the statement, they cannot formulate a question. NOTE: In some cases, the recovery force may be composed of non-U.S. forces.

10.4.1.2.3.6.6. Do not reference information that is public knowledge or can be found in the individuals military records.

10.4.1.2.3.6.7. Do not use culturally sensitive information.

10.4.1.2.3.7. Block 24, Additional Data. The theater JSRC or equivalent generally designates what is placed within this block. Some examples of data placed in this block include: type and date of SERE training received, ethnic group, allergies, clothing size, PRC-112

PLS code, Blood Chit number, etc. At the unit's discretion, this block can also be used to include data that didn't fit in other blocks, such as "Obvious Marks" from block 7.

10.4.1.2.3.8. Reverse side.

10.4.1.2.3.8.1. Fingerprinting will only be accomplished by qualified personnel.

10.4.1.2.3.8.2. Photographs of the individual will be taken while in normal mission uniform and without headgear. Since CSAR operations typically take place during combat operations, uniforms must be sanitized for these photos.

10.4.2. Digital ISOPREPs. The second format for creation/maintenance of ISOPREPs is to digitally store ISOPREP data. The AMC Digital ISOPREP was developed and fielded by AMC/IN, and approved by JPRA. This database is integrated into the AMC Phoenix Resource program, allowing secure, worldwide unit access while maintaining maximum data integrity. For the most part, the digital form is identical to DD Form 1833, except that there is no reverse side and fingerprints are not required. All of the standards defined for the hard-copy ISOPREP generally apply to the Digital ISOPREP, as well. Notable differences are defined below.

10.4.2.1. The AMC Digital ISOPREP is a single-page, electronic form.

10.4.2.2. In addition to textual identification and authentication data, front and profile view digital photographs are included on the front of the single-page document.

10.4.2.3. The AMC Digital ISOPREP program has no capacity to include fingerprints. As of the publication date of this handbook, JPRA had determined that fingerprints are not required on digital ISOPREPs.

10.4.2.4. ISOPREP data is stored on the AMC/IN Intelink-S server (**http://www.amcin.scott.af.smil.mil**). Access to the data is controlled via the unit's Phoenix Resource account login. Because connectivity to the server can potentially be interrupted, units must maintain two hardcopies of this data.

10.4.2.5. Unit personnel may access their unit's Digital ISOPREP records via a common web browser (i.e. Internet Explorer, Netscape Navigator, etc.). This scheme provides worldwide on-line access, as long as the user has a classified workstation, SIPRNET connectivity, a web browser, and access to their Phoenix Resource account.

10.4.2.6. When unit personnel deploy, their ISOPREP records can be placed into a "Deployed" status. While in deployed status, other AMC units can retrieve these records by searching the database for the individual's name, SSAN, or unit of assignment. If the member is deploying to a location without AMC support, his/her ISOPREP record may need to be emailed or secure faxed to the supporting location, as non-AMC units don't have access to the AMC ISOPREP database.

10.4.2.7. ISOPREP records can be permanently transferred to another unit when the member is reassigned within AMC. The losing unit initiates this process through the "Transfer ISOPREP" function available on the Digital ISOPREP main menu. By transferring the ISOPREP record, the losing unit changes the "data manager" assigned to that record from their own ISOPREP account, to the account of the gaining unit. Prior to affecting this change in ownership, the losing unit should coordinate with the gaining unit so that all concerned know that the action is taking place.

10.4.2.8. When needed by rescue authorities, ISOPREP records can be delivered one of two methods. E-mailing the digital ISOPREP record, or, (if connectivity is not available), faxing the hardcopy ISOPREP via secure fax.

10.4.2.9. The Digital ISOPREP Database tracks ISOPREP review dates and prompts the unit manager when review is due/overdue. This prompt is provided on the main menu screen of the Digital ISOPREP system, below the other primary system options.

10.4.2.10. AMC is scheduled to migrate their Phoenix Resource digital ISOPREP database to the Joint Personnel Recovery Agency's new software system, called Personnel Recovery Mission Software (PRMS). Introduction of JPRA's PRMS is yet to be determined. Units are encouraged to try out/train on the PRMS test site at **http://204.20.180.251/prms/** via the SIPRNET. To login, use 111-11-1111 as the SSN, and the password is password. DO NOT enter "real-world" info as anyone has access to the site. PRMS will have a download capability that will allow units to download the digital cards to the unit's own hard drive. This will allow units to have a digital backup in the event that connectivity is lost.

10.4.3. Transport of ISOPREP Cards. Members must never carry ISOPREP information with them on an employment mission into a tactical area of operation. Members of an aircrew or ground team in transit from home base to a deployment location may only transport ISOPREP forms, (as part of a classified courier package), if the package is dropped off at a staging location prior to entering the tactical area of operations. For example, a CONUS based aircrew flying from Charleston AFB to Tuzla AB would drop off the package at Rhein Main AB enroute. If hand carrying the ISOPREP cards in not feasible, home intelligence flights will mail them to the FOL through appropriate means.

10.4.4. Evasion Plan of Action. The EPA is another critical document used in the recovery process. An EPA is a document that tells recovery forces what the member plans to do if he/she becomes isolated. Recovery forces use the information in the EPA to determine where the evader will most likely be at any given time. Potential evaders must develop a tailored EPA prior to each mission. While intelligence, life support, and SERE personnel assist in the development of an EPA, the plan must be developed by the person whose recovery and survival will depend on the information provided. Although theater guidance may dictate format and contents for EPA's, minimum information required in an EPA may be found in JP 3-50.3, *Joint Doctrine for Evasion and Recovery*. Ensure you are familiar with theater guidance prior to departing on a deployment.

10.4.4.1. An EPA should be developed by the potential evader with the assistance of intelligence/SERE personnel and should be based on a thorough knowledge of the environment where isolation may occur. Evaders may gain such knowledge by studying the combat environment and the hostile territory before executing the mission, and by preplanning their evasion when they have the time to thoroughly analyze available options, therefore, ensure that the crew member prepares the EPA prior to the day of the mission. An EPA should address evasion plans from each point along the mission route. Plans should also address foreseeable contingencies, such as modifications due to injury, plans to evade as teams, or as individuals, etc.

10.4.4.2. EPA Development. The following information should be considered in the development of an adequate EPA (taken from Joint Pub 3-50.3, *Joint Doctrine*):

10.4.4.2.1. Identification. Include name and rank of each crew or team member. Also include mission identification data, such as mission number, aircraft or team call sign, crew or team position, type of aircraft, etc.

10.4.4.2.2. Planned Mission Flight Route or Delta Points. If not on file, the route points must be described in the EPA for both ingress and egress. Describe in-flight emergency plans for each leg of the mission.

10.4.4.2.3. Immediate Evasion actions and/or Intentions for the First 48 Hours (Uninjured.) Description of what the member will do during the first 48 hours. Under some conditions, the member may plan to hole-up near the crash site or parachute land site and wait for rescue. They may intend to evade a specified compass heading from the crash site for a certain distance and wait for contact. This section should also include a description of intended actions and length of stay at initial hiding location and address foreseeable contingencies that may impede these plans. The information entered here will most likely determine where recovery forces first attempt to contact the evader.

10.4.4.2.4. Immediate Evasion Actions and/or Intentions for the First 48 Hours (Injured.) This is a serious consideration for each mission leg. Even relatively minor injuries can significantly impact a member's ability to travel in difficult terrain or heavily controlled territory, and may dictate a completely different plan of action than if uninjured. The member needs to provide a plan that addresses issues of hiding, evading, traveling, etc., if injured. When initial post-isolation contact is made, the member must inform recovery forces of his/her physical condition.

10.4.4.2.5. Extended Evasion Actions and Intentions After 48 Hours. The member should consider the possibility of a long-term evasion situation and convey his/her ultimate intentions in such a scenario. Details should include ultimate destination, (i.e., a mountain range, a neighboring country, etc.), travel routes and techniques, intended contact points along the way, contact signals for recovery forces to look for, and back up plans.

10.4.4.2.6. Other information required on the EPA is generally provided by other personnel, but must be studied and completely understood by the potential evader. Communication and authentication procedures are usually published in the CSAR SPINs. Communication schedules and frequencies, SAR letter, number, color of the day, base headings, base altitudes, and other code procedures may also be used. Survival and communications gear available to the potential evader should also be listed in the EPA.

10.4.4.2.7. The following "checklist" may be helpful in developing a good EPA construct.

Step 1 - Determine Crewmember Responsibilities

- Group composition/Leadership
- Group leaders vs. Team leaders
- Security**,** classified destruction
- Cover, concealment, and camouflage
- Equipment
- Level of training
- Treatment, disposition of wounded

Step 2 - Immediate Actions upon Ditching or Bailout

- Will crew regroup, evade individually, or break into evasion teams?

- Location of initial evasion point
- Initial and extended evasion movement goals, techniques, and timelines
- Condition of evaders
- Length of stay near crash area (if no threat)
- Destruction of classified or sensitive materials

Step 3 - Evasion Movement (general)

- Individual positions or group movement
- Navigation responsibilities
- Security
- Noise/Light
- Camouflage
- Enemy sighting or contacts
- Danger areas
- Border crossings or recovery site
- Day or night movement

Step 4-Evasion Movement (specific) for Ingress, Objective Area, and Egress

- Enemy situation
- Detriments to travel
- Border situation
- Recommended travel routes
- Areas of chemical, biological, or radioactive activity
- Special evasion equipment and techniques
- Potential sources of food and water

Step 5-Selected Area for Evasion Intelligence Description (SAID), Selected Area for Evasion (SAFE), and E&R Areas

- General location and category
- Distinctive features
- Significant terrain features
- Contact points and procedures
- Intentions at contact point

Step 6-Evasion Communications

- Inventory of radio and signaling devices, and plans for use
- Phonetic designators for each team member
- Time schedule for contact among team members
- Secure communications procedures to be employed (hand signals, panels)

Step 7-Combat Search and Rescue (CSAR) Contact Procedures

- Radio and signaling devices to be used
- Call sign and frequency
- Time schedule for pre-contact and monitoring
- Alternate plan in heavy electronic threat environment

Step 8-Final Review. Freedom or captivity may well depend upon the ability to develop an effective EPA. Ensure you obtain a detailed review, briefing on:

- Geneva Convention
- Code of Conduct
- Legal Status
- Isolated Personnel Report (ISOPREP) Card Review
- Essential elements of information (EEI) Usage

10.4.4.2.8. JPRA's PRMS will also include an EPA shell with appropriate theater-specific data. Units are encouraged to go ahead and gain familiarity with the test site to help expedite "real world" use of the site when it comes on-line. The site can be accessed through the SIPRNET at **http://204.20.180.251/prms/**.

10.4.4.2.9. A sample EPA worksheet might be similar to the one on the following page. Units can review and tailor this sample to meet their mission needs, or they can opt to use one of the multiple other EPA shells that are available on the SIPRNET. Units should be aware that different commands require different EPA formats, and should meet the theater-specific requirements.

EPA Worksheet

I. GENERAL

CALL SIGN _____ DATE _____

MISSION, TARGET NUMBER _____ UNIT _____

NAME (S) _____

II. PREPARATION

_____ Review your ISOPREP (Personal Authenticator Number and Statements).

_____ Review the appropriate SAFEs/SAIDs.

_____ Review SPINS for daily authentication, contact procedures, and latest evasion guidance.

_____ Retain Dog Tags and DD Form 2 (Identification Card).

_____ Sanitize uniform of scarves, patches, and stars.

_____ Remove all personal items (driver's license, credit cards, photos, etc.).

_____ Pre-flight your survival vest and E&R kit contents.

III. IMMEDIATE ACTIONS AFTER BAILOUT, CRASH LANDING

A. INITIAL EVASION GOALS: Location of initial evasion point. (Where are you going - ingress, target area, egress?) Travel checkpoints

_____

_____

_____

B. EVASION MOVEMENT PROCEDURES (GENERAL): Consider noise, day, night movement, camouflage, enemy sighting, danger areas, recovery sites or crossing borders.

_____

_____

_____

IV. LONG-RANGE GOALS FOR EVASION MOVEMENT (SPECIFIC)

A. DETRIMENTS TO TRAVEL: Difficult terrain, major rivers, heavily populated areas, lack of concealment, weather factors, day, night, etc. (When and how you will move.)

_____

_____

B. BORDER SITUATION: What is present condition of contiguous borders? Neutral, allied, or permissive borders, coastlines within evasion distance?

_____

_____

C. RECOMMENDED TRAVEL ROUTES: Water, concealment, attitude of population, low population density.

_____

_____

D. LIKELY AREAS OF CBR CONTAMINATION: Prevailing wind direction.

_____

_____

POTENTIAL SOURCES OF FOOD & WATER: Location, methods for obtaining.

_____

_____

F. ENEMY SITUATION: Force deployment, uniforms, appearance, and weapons, search and interrogation tactics, expected treatment, and recommended resistance techniques.

_____

_____

_____

V. SAFE: COMPLETE REQUIRED ITEMS FOR INGRESS, TARGET AREA AND EGRESS AS REQUIRED.

A. LOCATION AND CATEGORIES: Describe general location and categories of SAFE that afford best prospects for survival, evasion, and recovery. Describe planned method for making contact with E&R net, if applicable (i.e., how will you let the net know you are in the area?)

INGRESS: _____

_____

_____

TARGET: _____

_____

_____

EGRESS: _____

_____

_____

B. DISTINCTIVE FEATURES (AIR): Describe distinctive features of areas that will enable visual identification from the air.

INGRESS: _____

TARGET: _____

EGRESS: _____

C. SIGNIFICANT TERRAIN FEATURES: Describe significant terrain features of areas that will enable visual identification from the ground.

INGRESS: _____

_____

TARGET: _____

_____

EGRESS: _____

_____

D. CONTACT POINTS, PROCEDURES: Describe designated contact points, contact procedures, and intentions at selected areas.

INGRESS: _____

_____

TARGET: _____

_____

EGRESS: _____

_____

VI. SAR CONTACT PROCEDURES

A. CALL SIGN: _____ B. FREQUENCY: _____

C. RADIO LISTENING PERIOD: _____

D. RADIO TRANSMITTING PERIOD: _____

E. GROUND-TO-AIR SIGNAL (STROBE LIGHT, PARACHUTE ETC): _____

_____ PLACE, TIME: _____

F. AUTHENTICATION CODES:

(1) COLOR, LETTER OF THE DAY: _____

(2) COLOR, LETTER OF THE MONTH: _____

(3) OTHER: _____

_____

G. PHOTO RECOGNITION SYMBOL:

DAY, TIME _____ NIGHT, TIME _____

H. SEARCH AND RESCUE NUMERICAL ENCRYPTION GRID (SARNEG)_____

0 1 2 3 4 5 6 7 8 9

VII. **ADDITIONAL COMMENTS**: Additional information regarding individual E & R plans, attitudes, and intentions should be attached to this EPA to assist search and rescue efforts should this plan ever be implemented. Give enough information to give planners an idea where to start looking. Local intelligence information can be included if such information is deemed reliable.

_____

_____

_____

* Relay codes are used by SAR forces to pass information (coordinates, movement in degrees, etc.) over an unsecured radio to an aircrew which is to be rescued. This code is not to be used to pass classified information. When preparing the EPA, choose a ten letter word you will remember and use as a letter/number replacement code, i.e. BLACKHORSE=0123456789. SAR forces can then tell the downed aircrew where they need to move using the letters that represent particular numbers, i.e., “move to ACBB North and BEKCB West.” The downed aircrew knows to proceed to 2300N09430W.

10.4.5. Escape & Evasion (E&E) Kits. E&E kits provide potential evaders with essential equipment, tools, and other items for successful evasion in specific, non-permissive environments. Their purpose is to provide the evader with the means to fix his/her position, navigate to a desired destination, evade and hide from the enemy, and signal recovery forces. They are designed to supplement/augment AF issued survival vest/kits. They should support the Joint Force Commander's PR plan by including items that aid in evasion and recovery and enhance the isolated person's ability to survive. They should be tailored to the specific unit, mission, and operating area to the maximum extent possible.

10.4.5.1. According to AFI 14-105, *Unit Intelligence Mission and Responsibilities*, the only item "required" in an E&E kit is an applicable Evasion Chart (EVC.) However, there are many other items that could, and should, be included in an E&E kit when possible, to include appropriate blood chits, Pointee-Talkees, daytime and nighttime signaling devices, and a button compass should be included. Other items to consider include barter items, Global Positioning System (GPS) receivers, infrared lights, camouflage netting, etc. Many times, the Joint Force Commander will direct, via the CSAR SPINS, that specific items be included.

10.4.5.2. Creative thinking will generate an E&E kit that contains all sorts of useful gadgets and devices. However, the specific size and placement of the kit on personnel should be closely scrutinized. Safety must be considered and balanced with the perceived usefulness of some items. If the kit becomes too large and cumbersome, it will likely never make it out of the plane. Additionally, exiting an aircraft in flight is a dangerous proposition under the best of circumstances. Adding a bulky item on the jumper's body can only further complicate the issue. As with all Personnel Recovery issues, be sure to fully coordinate with SERE and Life Support specialists.

10.4.6. Blood Chits.

10.4.6.1. A Blood Chit is a small sheet of material on which is printed an American Flag, a statement in English and several languages spoken by the populace in the operational area, and like numbers in each corner that identify the particular chit. The Blood Chit identifies the bearer as an American and promises a reward to anyone providing assistance to the bearer and/or helping the bearer to return to friendly control. When presented and properly validated, the Blood Chit represents an obligation of the U.S. Government to provide compensation for services rendered to isolated personnel. **Guidance for Blood Chit use is found in Joint Publication 3-50.3, classified appendix G. The JPRA Blood Chit Program policy can be found on the AMC SIPRNET homepage under Intel Products/Other Escape & Recovery Products.**

10.4.6.2. Blood Chits are controlled items, and must be treated as such. The JPRA is the Office of Primary Responsibility (OPR) for Blood Chit policy and for authorizing the production, distribution, and use of Blood Chits. JPRA maintains a master control record for all Blood Chits issued to Command/Theater Blood Chit Managers. Units order Blood Chits from either AMC/INXU or the Theater Blood Chit manager, depending upon circumstance. If a unit is deploying and will be CHOP'D to another MAJCOM, except for EUCOM, then it should order the required Blood Chits from the Theater Manager. If the unit is deploying but will not be CHOP'D, or is deploying to EUCOM, then it should order the Blood Chits thru AMC/INXU. The quantity and serial numbers issued to units must be signed for and the receipt returned to the appropriate Blood Chit Manager. Units maintain a record of the Blood Chit serial number and series issued to each individual. If Blood Chits are pooled, a record must be kept each time they are issued. They should only be issued prior to combat missions and deployments to high threat areas, and should be collected and properly stored immediately after completion of missions. Blood Chits must be returned to AMC/INXU or the Theater Blood Chit manager at the conclusion of operational requirements. The manager will then ensure proper accountability and that the return receipt is forwarded to the user.

10.4.6.3. The Command/Theater Blood Chit Program Managers are:

AMC/INXU - DSN: 779-4455

USCENTCOM - USCENTAF/A3-DOOR, DSN: 318-965-2957

USEUCOM – USAFE 32 AOS/AOOR, DSN: 314-480-6885/9713

USPACOM – PAC/RCC, DSN: 315-449-2268

USSOCOM – AFSOC/DOXJ, DSN: 579-3293

USSOUTHCOM – JSRC, DSN: 483-5830

USAF – ACC – ACC/DOTO, DSN: 574-8165

10.4.6.4. AMC Units will not store/maintain Blood Chits at home station unless it is in preparation for forward deployment. When a unit is notified of a pending deployment to an area that requires Blood Chits, they should get in contact with the appropriate Blood Chit manager (reference paragraph 10.3.6.2) and order the required amount of Blood Chits. There is no set equation that will work every time on the correct amount of Blood Chits to order, but common sense needs to prevail. Rule of thumb is to add one extra jet to any equation. So, a unit deploying that will be supporting 5 KC-10's with ten crews (2 crews per jet) needs to order 48 Blood Chits (10 crews x 4 members per crew + 8 for the additional ghost jet.)

10.4.6.5. The loss or theft of Blood Chits is subject to appropriate investigation as a controlled item. The report of loss or theft (specifying the Blood Chit serial number, the Blood Chit series, and the unit of assignment), along with a report of investigation and a determination/reason for the loss or theft will be forwarded to the Command or Theater Program Manager and the JPRA as soon as possible after the loss/theft is discovered. All individuals participating in the Blood Chit program need to be reminded that Blood Chits are controlled items – Government property, and are NOT souvenirs.

10.5. Downed Aircrew Procedures.

10.5.1. When notified that one of your aircraft is down, lost, or otherwise missing, it becomes extremely important that the ISOPREP and EPA data for the crewmembers be immediately forwarded to rescue authorities. Specific policy and procedures will be directed by the Joint Recovery Coordination Center (JRCC) via the CSAR SPINS, but you should always be prepared to exercise flexibility to get the information to where it's needed.

10.5.2. ISOPREP and EPA data for all crewmembers on a specific aircraft engaged in a mission should be maintained as an integral package and readily available for immediate transfer to rescue authorities. When the crew returns from the mission, their products can be filed back into your normal filing scheme. Should the unit receive word that an aircraft is missing, ISOPREP and EPA data must be immediately transferred to the JRCC via the most expeditious, secure means available.

10.5.3. The following checklist can be used for most Downed Aircrew situations.

CHECKLIST		PAGE 1 OF 1 PAGES		
TITLE/SUBJECT/ACTIVITY **DOWNED AIRCREW**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
	1. Immediately contact theater Joint Search and Recovery Center (JSRC). Transmit all aircrew ISOPREPs (DD Form 1833) by quickest means possible as per ATO/SPINs. 2. Contact Command Post/WOC ASAP and be prepared to provide as much of the following information as possible, for inclusion into the OPREP-3 and LOSREP: A. Operation name or type of occurrence (operational, combat, or training). B. Type aircraft/Tail number/Call Sign. C. Unit/Operational base/Home base of aircraft. D. Mission number/type (AR, cargo, or pax). E. Time and location when aircraft was downed, lost, or crashed. F. Description of all known facts/circumstances (altitude, attitude, speed, EW, threats, tactics/etc). G. Weather conditions at time and place of incident. H. Aircrew identification (name, rank, SSN), estimate of casualties, names of VIPs involved I. Rescue information. J. Description of material and circumstances of any possible compromise of classified material. K. Remarks: Any other essential information you may have.			

NOTE: The OPREP-3 and LOSREP are operational reports. Provide the information to the local JSRC/Command Post/DIRMOBFOR/AOC ASAP, but be sure to forward the information to HQ AMC/IN as soon as time permits. DO NOT DELAY REPORTING TO RESEARCH ADDITIONAL INFO. IMMEDIATELY TRANSMIT WHAT YOU KNOW! 3. Brief information to all follow-on missions and other applicable agencies as necessary. 4. Plot incident on main situation board and update as often as possible.			

10.6. Critical Personnel Recovery References. The following documents should be maintained, read, and used as primary references for developing and maintaining your unit's PR Support Programs.

10.6.1. Joint Publications (Unless otherwise noted, available on SIPRNET at **http://www.jpra.jfcom.smil.mil/products/pubs.htm**).

- DoD Directive 1300.7, Training and Education Measures Necessary to Support the Code of Conduct (**http://www.dtic.mil/whs/directives/**)
- DoD Directive 2310.1, Personnel Recovery (**http://www.dtic.mil/whs/directives/**)
- CJCSI 3270.01, Personnel Recovery within the Department of Defense (Classified)

- Joint Pub 3-50.2, Doctrine for Joint Combat Search and Rescue
- Joint Pub 3-50.3, Joint Doctrine for Evasion and Recovery
- Joint Pub 3-50.21, Joint Tactics, Techniques, and Procedures for Combat Search and Rescue

10.6.2. Air Force Publications (Available at **http://www.e-publishing.af.mil/**)

- AFDD 2-1.6, Combat Search and Rescue
- AFI 16-1301, Survival, Evasion, Resistance, and Escape Program
- AFI 11-301V1, Aircrew Life Support Program
- AFI 14-105, Unit Intelligence Mission and Responsibilities
- AFI 16-1301, Survival, Evasion, Resistance, and Escape (SERE) Operations and Program

Chapter 11

SECURITY

11.1. General. This chapter contains information and procedures everyone must understand and practice to fulfill security responsibilities. It does not replace governing security instructions, but you can use it as a ready reference. Your supervisor, security manager, and base Information Security Program Manager (ISPM) are also able to assist you if you have security questions. For all questions regarding SCI, consult your local Special Security Representative (SSR), SSO or call USTRANSCOM/TCJ2-S at DSN 779-6965.

11.2. Reference Documents. You are responsible for protecting information which, if put in the wrong hands, could be a detriment to national security. As authorized custodians of classified information, we must follow the principles of need to know, proper identification, and proper clearances. In your capacity as briefer, aircrew trainer, and guardian of classified information, you are required to apply proper security measures on a daily basis. It is your duty to protect classified material. To ensure compliance with these requirements, you must be intimately familiar with the following publications:

- DoD 5200.1-R, *Information Security Program*
- DoD 5200.2-R, *Personnel Security Program*
- AFI 31-401, *Information Security Program Management*
- AFI 31-406, *Applying the North Atlantic Treaty Organization (NATO) Protection Standards*
- AFI 31-501, *Personnel Security Program Management*
- AFI 33-202, *Computer Security*
- AFI 33-203, *Emission Security*
- AFI 33-209, *Operational Instruction for the Secure Telephone Unit (STU-III) Type 1*

11.3. Information Security (INFOSEC) Program. Your commander administers the Information Security Program via a security manager. Your security manager is your most important contact when dealing with security guidelines and problems. One of the biggest responsibilities of the security manager is to assure an active and effective training program is in place. While your security manager may not be the focal point for all related security training, he/she should give you guidance on areas covered by the security-training program. While everyone requires some security education, those in the intelligence career field need more than a fleeting understanding of security measures. Review the following topics as an introduction to your information security training.

11.3.1. Protection of Classified Information. As a custodian of classified information, you have a personal, moral, and legal responsibility to protect classified information, oral or written, at all times. You must understand and continually practice correct handling, protection, and storage procedures. You'll need to be aware of unique requirements for items such as typewriter ribbons and diskettes. Your responsibilities also include locking classified information in appropriate security containers whenever it is not in use or under the direct supervision of authorized persons. Further, you must follow procedures that ensure unauthorized persons don't gain access to classified information. These procedures include:

11.3.1.1. Before you leave the office, properly secure all classified material. Never leave classified material unattended. Store classified materials only in GSA approved security containers. Be sure you properly dispose of all classified waste material as unattended classified material represents a compromise risk.

11.3.1.2. Avoid unnecessary reproduction of classified material. Reproduced classified material is subject to the same control as the original document. Do not reproduce classified material without authorization from an official designated to grant such approval. Do not reproduce Top Secret material without the consent of the originator or higher authority.

11.3.1.3. Do not discuss classified material on a standard telephone. Don't be fooled by telephone callers who drop names or otherwise try to impress you with urgent needs. Speaking in private codes or talking around classified information doesn't really fool anyone and is strictly prohibited.

11.3.2. Disclosure.

11.3.2.1. Authorized Disclosure. No one has a right to have access to classified information solely because of rank or position. The final responsibility for determining whether an individual's official duties require possession of, or access to, classified information rests upon the control of the information and not upon the prospective recipient.

11.3.2.1.1. Disclose classified information only to authorized individuals. Don't assume anything. Check identity, need-to-know, and the ability of the individual to properly protect the information. Use Joint Clearance Access Verification System (JCAVS) to verify clearance and a signed nondisclosure agreement, before releasing the information.

11.3.2.1.2. Be aware of open doors, windows, telephone lines, etc., before you discuss classified information. Authorized personnel may be in the room, but unauthorized personnel could be nearby. Remember the clean-desk policy when departing for the day and make an end-of-day security check of your work area.

11.3.2.1.3. Report any attempt by unauthorized personnel to obtain classified information to your supervisor, security manager, commander, or information security representative.

11.3.2.1.4. Finally, strictly limit distribution of papers containing classified information. When in doubt, DO NOT send it. Avoid routine dissemination of classified material. Remember, a disclosure record that lists every person who had access to the document must accompany each Top Secret document.

11.3.2.2. Unauthorized Disclosure. Unauthorized disclosure of classified information can easily result in damage to our national security and/or the security of ongoing or planned operations. Lives could be at stake. Therefore, unauthorized disclosure may result in disciplinary or legal action. Such action may include a warning notice, formal reprimand, suspension without pay, forfeiture of pay, court-martial, discharge, fine and/or imprisonment.

11.3.3. Hand-Carrying Classified Material. Each installation you visit or from which you operate will have specific procedures and requirements regarding hand-carrying classified information; however, the basic elements of these procedures are normally fairly consistent. Do not hand-carry classified material outside the normal work area without prior approval. Ensure classified material is properly secured within an appropriate carrying device (folder, envelope, briefcase, etc.) when hand-carrying outside of a building. When hand carrying classified material off the installation, more stringent pro-

cedures apply. If designated an official courier, obtain training concerning these procedures. Before couriering SCI documents, contact your servicing SSO for requirements, procedures, and training.

11.3.4. Reporting Security Violations/Incidents.

11.3.4.1. If you become aware of a security incident, either collateral or SCI, promptly report it to either your security manager, servicing SSO, or people listed on Standard Form 700, *Security Container Information* (normally posted inside the safe's locking drawer or on the vault door). Always protect unsecured classified information until the responsible custodian gains custody. When the commander or staff agency chief becomes aware of a security incident, he or she will appoint a person to conduct a preliminary inquiry. Preliminary inquiries determine:

- Whether or not a security incident occurred.
- The type of violation.
- The source and reason for the security incident.

  The appropriate measures or actions to minimize or negate the adverse effect of the security incident.
- Necessary changes to ensure the same type violation does not recur.

11.3.4.2. An inquiry is not extensive in scope; it gathers available facts to support conclusions or recommendations made by the inquiry official. Upon receipt of the written inquiry report, the appointing authority reviews the report and takes administrative or disciplinary action as appropriate. Local SF authorities then determine whether a formal investigation is required. Most Air Force INFOSEC incidents are closed without a formal investigation.

11.4. Computer Security (COMPUSEC).

11.4.1. COMPUSEC is the component of the Information Protection discipline that measures, controls, and protects data in a computer against unauthorized (accidental or intentional) disclosure, modification, or destruction. COMPUSEC includes the consideration of all hardware and software, operational and accountability procedures, and access controls at a central computer facility, remote computer, or terminal. It also includes management constraints, physical structures and devices, and personnel and communications controls needed to provide an acceptable level of risk for the computer systems, and the data they contain.

11.4.2. Every Air Force C4I system has vulnerabilities that make it susceptible to exploitation. To reduce these vulnerabilities we use countermeasures to a level that, when compared to the threat, equals an acceptable risk.

11.4.3. Three threats of particular concern in today's Air Force are intrusion by computer hackers; the introduction of malicious logic (viruses, Trojan horses, trapdoors, and worms) into computer systems; and Fraud, Waste, and Abuse (FW&A) of computer resources.

11.4.3.1. Computer Hackers. Hackers are normally personal computer users who develop a curiosity about the C4I systems' world. These individuals break into computers for various purposes. Most involved casual browsing of the systems, but some hacker intrusions include downloading of password files and introduction of malicious logic. In recent years, the number of intrusion

attempts into Air Force systems has been on the rise. There is a twofold reason for this increase in computer incidents. First, the number of hackers is on the rise. Second, computer security professionals are becoming better at protecting their systems and data--attempting to close the door to hackers by denying access, identifying access attempts and actual penetrations, and reporting the incidents to the proper agencies.

11.4.3.2. Malicious Logic. The largest and most prevalent threat to C4I systems is malicious logic injected into a computer system for a specific mission such as destruction or manipulation of data files. Malicious logic, commonly known as computer viruses, is infecting Air Force computers in increasing numbers. This increase is largely due to typically poor COMPUSEC practices such as downloading unauthorized and/or untested software for use on government systems, accessing or transferring data files from computer bulletin boards and the Internet that are not virus scanned, using removable media (i.e., floppy disks) that have not been virus scanned and not updating virus detection software signature files on a regular basis. The prevalence and potential for viruses to infect computer systems grows every day as new viruses are introduced, as people share computers, software programs and gain access to mainframes, servers, and networks. C4I systems users must report incidents (hackers and malicious logic) to their Computer Systems Security Officer (CSSO).

11.4.3.3. Fraud, Waste, and Abuse (FW&A) of Computer Resources. FW&A results from any intentional deception designed to unlawfully deprive the Air Force of something of value or to secure an entitlement such as a benefit, privilege, allowance, or consideration for an unauthorized individual. FW&A can also result from the careless or needless expenditure of Air Force funds or resources, or the intentional, wrongful, or improper use of computer resources. All personnel that use or have access to computer resources must safeguard the resources and prevent FW&A.

11.4.4. Your Role in the Air Force COMPUSEC Program. First and foremost, ensure all your computer systems are accredited! You must recognize that the threats are real and ensure the proper use of COMPUSEC countermeasures. Failure to reduce the vulnerabilities to the lowest possible level could result in the loss of life, critical weapon systems becoming inoperative or missing their targets, the compromise of classified war plans, the loss of thousands of dollars in computer time and work hours, or the destruction of valuable information. Computer users must reduce the risks to the lowest level possible. Report deviations from security practices and FW&A violations to the information systems security officer, commander, or to the Air Force Office of Special Investigations (AFOSI).

11.5. Communications Security (COMSEC).

11.5.1. Why we need COMSEC. We know that every major nation in the world is trying to collect intelligence from other nations they oppose politically, economically, and militarily. Even unclassified information, when collected over time, from a variety of sources and locations, can reveal details concerning an opponent's activities. These details can include operations, plans, programs, strengths, weaknesses, numbers, equipment, deployment, capabilities, and intentions. In the hands of trained analysts, virtually any information can be of intelligence value, either alone or when pieced together with other collected information. When in doubt, “go secure” on a STU-III/STE, if even to discuss unclassified information. Much intelligence is gleaned from phone calls prior to the “turning” of the STU/STE key. The enemy is listening.

11.5.2. COMSEC Defined. COMSEC entails all measures taken to deny unauthorized persons national security information derived from the telecommunications of the US Government. COMSEC

also ensures the authenticity of telecommunications. Telecommunications refer to the preparation, transmission, or processing of information by electrical means. Protective measures under COMSEC include crypto-security, transmission security, emission security, and physical security of COMSEC material and information.

11.5.3. COMSEC Physical Security. Physical security results from taking all physical measures necessary to safeguard classified equipment, material, and information from access or observation by unauthorized persons. Everyone in the Air Force who works with classified information must use physical security measures. Examples of COMSEC physical security measures are:

- Properly securing cryptographic and other COMSEC materials through the use of armed guards or approved containers.
- Ensuring only authorized persons have access to COMSEC material.
- Ensuring COMSEC materials and procedures are used in strict compliance with applicable directives.

11.5.4. Crypto-security. Crypto-security is the proper use of technically sound cryptographic systems. Anyone using cryptographic equipment, codes, ciphers, authentication systems, and similar materials must:

- Adhere to the operating instructions and procedures (which accompany every cryptographic device or material) in the encryption of information.
- Never mix codes or encrypted text with plain message text, unless specifically authorized by the controlling authority for the encryption device/material.
- Never discuss the encryption or decryption process outside a cryptographically secure area or over an unsecured telephone.

11.5.5. Transmission Security (TRANSEC). TRANSEC results from all measures designed to protect transmissions from interception and exploitation by means other than crypto-analysis (code breaking). Everyone in the Air Force must practice TRANSEC because, as a minimum, we use the telephone in the performance of our duties. Some examples of TRANSEC include:

- Using registered mail and secured communications for transmitting classified or sensitive unclassified information.
- Using cryptographically secured telephone, such as a STU-III, and/or approved Emission Security (EMSEC) facsimile equipment.
- Correctly using authorized manual crypto systems, call signs, or authenticators when using unsecured telephones or radios.
- Never attempting to "talk around" classified subjects or using homemade codes or references to pass classified information by unsecured communications.

11.6. Emission Security (EMSEC).

11.6.1. EMSEC (formerly known as TEMPEST) refers to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment.

Compromising emanations are unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by classified processing equipment. When we operate computers, facsimiles, voice or record communications, or other electronic information processing systems, they emit electromagnetic signals. These signals, although unintentional and normally of fairly low power, radiate like radio waves along different paths. They escape to free space through conduction along power cords, the electrical distribution system, or coupling with nearby objects such as telephones, telephone lines, water pipes, or air ducts. We refer to these signals, which reveal the processed information, as emanations.

11.6.2. The actions required to detect and exploit compromising emanations are passive and covert; therefore, we must apply effective countermeasures to reduce these risks. Naturally, cost plays a significant part; the countermeasures selected should achieve the EMSEC protection required as determined by an Emission Security Countermeasures Assessment. Whenever you are planning to move classified equipment or replace old equipment with new equipment, contact your local EMSEC office for collateral systems, or your servicing SSO for SCI systems, for an Emission Security Countermeasure Assessment prior to any equipment movement or installation.

11.6.3. The commander of every installation must appoint an EMSEC officer. You, as a system end-user, are responsible for ensuring that you comply with all applicable EMSEC requirements, no matter where you are. Find out who your installation EMSEC officer is and direct any/all questions regarding equipment placement and assessments to that person for collateral systems. For SCI systems, your first stop should always be your servicing SSO.

11.7. Operations Security (OPSEC).

11.7.1. OPSEC is a broader based security program designed to prevent all types of sensitive information (often unclassified) from getting into the wrong hands. Such information can be extremely valuable to our adversaries because it can provide intelligence indicators of our daily operations and, more importantly, our future plans and activities. OPSEC is the process of denying adversaries information about USAF capabilities and intentions by identifying, controlling, and protecting indicators associated with the planning and conduct of military operations or exercises. The key to successful OPSEC is identifying indicators that are tip-offs of impending activities, such as repetitive standard operating procedures or in some cases, observable deviations from normal operations. For example, unusual changes in duty hours, large numbers of TDY personnel to or from a unit, or increased aircraft sorties launched in a given time period could be valuable clues to an adversary. Remember: Our adversaries don't necessarily need to know when or where we plan to conduct certain operations; however, they do need information concerning our capabilities and intentions so they can plan their war fighting strategies.

11.7.2. The OPSEC Process. OPSEC is a continuous, systematic process involving security and common sense. We use it to analyze Air Force operations plans or programs to detect any weakness that may be providing our enemies insights into our mission. The most important steps in the process are:

- Knowing your unit's mission.
- Recognizing the adversary intelligence threat to your unit.
- Being aware of your unit's critical information - Essential Elements of Friendly Information (EEFIs).

- Identifying indicators that might disclose this information.
- Developing protective measures to eliminate these indicators, thereby denying our adversaries the information they need to plan operations against us.

11.8. AMC Foreign Disclosure Program .

11.8.1. HQ AMC/XPRI-FDO is the Command Foreign Disclosure Office (FDO) and Designated Disclosure Authority (DDA) for AMC. All requests for disclosure or release of AMC information (classified and controlled unclassified) to a foreign representative must be submitted to HQ AMC/XPRI-FDO. Disclosure implies "oral and visual" information and release implies "documentation." AMC discloses/releases information to foreign nationals and their representatives through several different programs. Foreign nationals often visit AMC bases/units. Foreign national students attend AMC courses. We participate in exchange and liaison programs with foreign nations. We receive requests for AMC documents and information. AMC personnel often present information at conferences with foreign nationals in attendance. All of these examples require some level of foreign disclosure guidance. Key documents to be familiar with include:

- AFI 16-107, *International Personnel Exchange Program*. This document is available on the Air Force Publications (AFPUBS) home page.
- The AMC Supplement to AFI 16-107, *International Personnel Exchange Program*.
- AFI 16-201, *Disclosure of Military Information to Foreign Governments and International Organizations*. This is a classified document and not available on the AFPUBS home page.

11.8.2. Foreign National Access to Automated Information Systems. Before a foreign national can be granted access to an Automated Information System (AIS), a foreign disclosure review of the information on the system is required. AFI 33-202, *Computer Security*, paragraph. 3.7 applies.

11.8.3. Intelligence support to AMC foreign exchange officers. Intelligence personnel routinely brief foreign exchange officers assigned to AMC Units as aircrew members. Exchange officers do not have U.S. security clearances. The Delegation of Disclosure Authority Letter (DDL) for the position authorizes access to classified and controlled unclassified information. The intelligence unit supporting an exchange officer should be thoroughly familiar with the disclosure guidance for the position. Most exchange officers assigned to AMC are authorized access to current intelligence information up to SECRET. See the AMC/IN Foreign Disclosure web page on Intelink-S for additional information.

11.8.4. The AMC FDO maintains a Foreign Disclosure Information page on the AMC/IN Intelink-S web site. This page can be found under the "Support" menu item of the main page, or at URL (**http://www.amcin.scott.af.smil.mil/foreign_disclosure/fdmain.html**). Guidance contained on the FDO page includes:

- Specific guidance on the disclosure of intelligence information.
- Current listing of foreign officers assigned to AMC.

- Current listing of AMC Base/Unit Foreign Disclosure Officers
- AMC Foreign Disclosure Advisories

11.8.5. Any questions not answered by reviewing the FDO page and/or reference documentation should be directed to the AMC Foreign Disclosure Officer, Mrs. Donna Hubbard, HQ AMC/ XPRI-FDO, DSN 779-3518, STU III 779-6727, Unclas FAX: 779-4606.

Chapter 12

MOBILITY

12.1. General. This chapter provides information on the diversity of situations encountered in managing and supporting air mobility forces assigned to or operating within a combined or unified command theater or joint operations area.

12.2. Theater Force Management. Within a theater of operations, the Joint Forces Commander (JFC) is responsible for directing and coordinating all assigned and attached resources. The JFC commits the resources under his operational control to the respective component commanders in accordance with operational plans reflecting overall theater strategy.

12.2.1. The management of theater-assigned and attached air forces is the responsibility of the Joint Force Air Component Commander (JFACC) and Air Operations Center (AOC) director. However, Commander, Air Mobility Command (COMAMC) and Commander, Air Combat Command (COMACC) retain administrative command as appropriate.

12.2.2. The AOC director plans air mobility activities according to the requirements and complexity of the mission, and executes air mobility activities through the Air Mobility Division (AMD). The AMD is an extension of the AMC TACC for regional coordination/integration of AMC mobility and support resources in contingency, humanitarian, and wartime scenarios.

12.2.3. To assist with the management of theater airlift forces, the 621st Air Mobility Operations Squadron (AMOS) and 615 AMOS maintain a cadre of personnel to form the nucleus of an AOC/AMD. In garrison, these squadrons are available to assist headquarters and theater staffs in planning the management of air mobility forces for exercises/contingencies and coordinating with other agencies to meet operational objectives.

12.2.4. The AOC is the principal agency where the planning, coordination, and execution of theater air operations are accomplished. The AOC is divided into various functional divisions, one of which may be an AMD. Responsibilities of the AMD with respect to command, operations, logistics, transportation and intelligence are closely related to those of other AOC divisions.

12.3. Director of Mobility Forces (DIRMOBFOR). The DIRMOBFOR is designated by, and works for, the supported commander. The DIRMOBFOR serves as the theater commander's agent for all theater air mobility issues related to a specific joint or combined operation or exercise.

12.4. JFACC. The JFACC exercises operational control responsibilities through the AOC/AMD. The number, level, and size of subordinate units required to accomplish the mission may dictate the number of regional AOCs in a given theater. The AMD receives validated theater airlift requests and schedules the appropriate missions for them. The AMD assigns missions and the necessary air mobility resources to subordinate agencies. AMD duties include:

- Managing, coordinating, and directing theater-assigned and attached airlift, operational support, to accomplish all air mobility requirements.

- Establishing the appropriate theater mobility management organization (recommend AFCC establish provisional units, etc., as required).
- Ensuring air mobility related intelligence is collected, analyzed and disseminated.
- The AOC/AMD consists of all the functional areas required to manage air mobility resources within a theater of operations and must maintain the flexibility to enable tailoring to a multitude of environments.

12.5. Tactical Airlift Liaison Officers (TALOs). TALOs also assist the AMD and units. These rated officers have extensive experience in tactical airlift and airdrop operations. They are assigned to selected Army units with high priority short notice airborne and air mobility missions. They work with the supported commander's G-3/G-4 staff to provide advice and assistance on air mobility matters. They also assist in requesting tactical airlift and survey/approve tactical drop zones and control certain airdrop operations.

NOTE: Each theaters air mobility organization is unique. Augmentation forces must be prepared to operate within any theater air mobility organization. Additionally, during operations in the past, MAF units have often operated autonomously or as a part of larger MAF wings. Recent operations have shown that many times MAF units will be subordinate to CAF lead wings that include a variety of aircraft. This means that MAF intelligence personnel supporting squadron operations will need to utilize an intelligence support structure they may not be used to working with. When deployed to a CAF base, or when operating within a CAF command structure, it is important to facilitate cooperation in order to accomplish intelligence operations. Be aware that the CAF personnel may not be used to working with MAF units, or providing mission-required intelligence tailored to MAF assets. It is your responsibility to educate personnel at the deployed Wing and OSS on your unique intelligence needs, aircraft operations, and required support. By clearly articulating your requirements, you will get the support you need. Additionally, as the MAF squadron intelligence representative, you may need to learn AOR-specific procedures for intelligence reporting, briefing, and RFIs that will be standard across all deployed wings. This may include a different MISREP format and reporting procedures/requirements. Knowing these procedures prior to departure for the deployed location will allow you to train all personnel before arrival.

12.6. Manpower and Material.

12.6.1. Upon receipt of planning orders each unit builds a Manpower and Material (M&M) package. While preparing this package most units will require information or assistance from headquarters. Due to personnel shortages, economy of force is key. It is important to remember that air mobility units usually deploy using organic lift, thus, consideration should be given to take only the required equipment.

12.6.2. Send the M&M to headquarters for review. The M&M will list the UTCs required to complete the tasked mission as well as sourcing. Sometimes the unit cannot fill the UTC requirement internally; in those cases headquarters will source from other units. From the M&M the functional managers build a Deployment Manning Document (DMD) and task accordingly via an Air Mobility Tasking (AMT) message. This message should go out five days a week to every command post and wing plans shop. Tasking should also be accomplished through the personnel system, COMPES. Units will cut orders upon receipt of an official levy flow. HQ DP and XP should also receive a copy of the AMT and initiate the levy flow and update DMD, respectively. This same information is also used to update

the plan in Joint Operations Planning Execution System (JOPES). Units subsequently receive the tasking and coordinate the deployment with HQ AMC/INXX.

12.7. Prior to Deployment. Preparing your mobility documents, equipment, and supplies for deployment is one of your most important responsibilities.

12.7.1. Documents.

12.7.1.1. Review the SIDL and ensure the latest versions of all necessary documents are on hand.

12.7.1.2. Some units use colored tape, stickers, or a big "M" on the side of the binder to identify mobility documents. You must be able to easily retrieve them for short-notice tasking.

12.7.1.3. Upon notification to mobilize pull the appropriate documents according to OPLAN tasking. Multiple plans may require multiple colors.

12.7.1.4. Some units choose to put their documents in a safe, box, or footlocker, and eventually in a mobility bin or on a pallet instead of hand carrying them. If you choose this method, remember you must have a classified courier card to escort the pallet.

12.7.2. Maps and Charts. Just like you identify your mobility documents, you also need to identify charts used for mobility.

12.7.3. Supplies. Number-code each box/bin and create a reference sheet listing the contents of each box/bin. This will speed processing them in the mobility line, unpacking, and shop set-up at the Forward Operating Location/Base (FOL/FOB). It will enable you to access the items you need without looking through each box/bin.

12.7.4. Loading the Pallets or Bins. Always place heavier boxes on the bottom. Place classified material in an easily accessible location, in case of an emergency. If packing a bin, use the available space to the fullest extent to prevent slipping and settling during movement.

12.7.5. Weight and Cube. Once packing is complete, mark the containers with weight and cube (write the information on masking tape.) You must do this before turning over the bin to LG. Lock the bin with a Government Services Administration (GSA) approved padlock. If it contains classified, mark the bin "Exempt from Examination" and a courier must escort it at all times until it reaches its destination and the contents moved to a secure storage location.

12.7.6. Communications. Many steady state operations already have both classified and unclassified LANs and e-mail services set up. However, if deploying to an austere location, pre-coordinate and set-up accounts for both SIPRNET and NIPRNET prior to departure.

12.8. Operating At Deployed Location. There are numerous things to do upon arrival at the deployed location. They include: setting up the Intelligence shop, establishing schedules, finding out when and where the next missions go, etc. See the checklist on page 127 for additional information

12.8.1. Receiving Message Traffic at Deployed Locations. Receiving message traffic while deployed takes a little prep work before leaving your home station. Prior to deploying, units should contact their home station Communications Center. The Communications Center will assist in establishing your deployed Plain Language Address (PLA). Message originators will need the PLA to add you to their addressee list.

12.8.2. Picking Up Traffic at Deployed Location. A letter designating individuals to pick up message traffic must be filed with the deployed Communications Center. See example in attachment 5 of this chapter.

12.9. Intelligence and Tactics.

12.9.1. As a member of the intelligence community, unit intelligence shops should establish a good working relationship with the unit's tactics shop at home station and deployed. When it comes to giving your aircrews the best available information on threats and counter tactics, intelligence and tactics need to work hand-in-hand; establishing a good rapport with tactics will prove to be invaluable.

12.9.2. Tactics designs combat employment techniques. They act as overall mission planners, looking at the "big picture" of the contingency/exercise area. Intelligence can assist tactics by providing information on threats. Tacticians assist intelligence by explaining airframe systems, performance capabilities and limitations. They enhance intelligence’s credibility with the aircrews by providing us with an operator's perspective. During combat operations, the tactics section provides intelligence with specific route information and operational concerns.

12.10. Maintaining Logs. We highly encourage you to use logs or journals to document taskings and events. There are two types of logs you should maintain.

12.10.1. Daily events log. The events log is extremely useful, especially during shift changeover briefings. You can also use it to leave messages, incoming calls, unsolved problems, aircrew questions, urgent items, etc., providing a concise history of events.

12.10.2. Incoming/outgoing message log. This log provides a quick reference and accounting of all message traffic (Date-Time Groups (DTGs), topics, countries, etc.).

12.11. Checklists.

CHECKLIST		PAGE 1 OF 1 PAGES		
TITLE/SUBJECT/ACTIVITY **GENERAL MOBILITY - Coordinate with Mobility Officer or NCO**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
	1. Intelligence personnel: A. Have an up-to-date shot record. B. Confirmed eligible for deployment by the Unit Commander/Mobility Officer. C. Issued mobility gear IAW Wing Mobility Annexes. D. Receive necessary mobility training (weapons, self-aid buddy-care, theater specific training, etc). E. Issued the Unit Mobility Processing Checklist. F. Checked to ensure proper clearance or eligibility. G. Established deployed SIPRNET, NIPRNET, JWICS e-mail accounts (if applicable). 2. Mobility POC notifies appropriate wing agencies on new mobility members. 3. Assemble mobility kits to fulfill deployment requirements as stated in tasked Unit Type Codes (UTCs). 4. If there are mobility kit shortages, place order. 5. Develop deployment Operating Instructions (OIs) and checklists covering all actions for deployed and home station personnel. 6. Establish checklists covering employment and implementation procedures at the FOL.			

CHECKLIST		PAGE 1 OF 3 PAGES		
TITLE/SUBJECT/ACTIVITY **INITIAL DEPLOYMENT SITE (FOL/FOB)**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
	1. Arrival: A. Have arrangements been made for office/work area? (1) Is it large enough to display maps? (2) Does it have sufficient briefing/mission planning space? (3) Is it close to or collocated with Current Ops and Tactics? (4) Has space been set aside or designated for debriefings? (5) Is the area securable? (6) Is access to the area limited; access roster accomplished? B. Have you made arrangements to store classified until your field safe arrives? C. Communication Arrangements: (1) Have you made arrangements for voice communications (Both secure and unsecure)? (2) Have you made arrangements for message communications: (a) Location of Comm Center? (b) Pick up of message (who and how)?			

	(c) Delivery of messages (who and how)? (3) Deliver letter to site Comm Center authorizing Intel personnel to deliver/receive messages. D. Have you made arrangements for pallet pick up and delivery? E. Have you made arrangements for transportation? (1) Pick-up of newly arrived personnel? (2) Daily work/message delivery/debriefs, etc.?			

CHECKLIST		PAGE 2 OF 3 PAGES		
TITLE/SUBJECT/ACTIVITY **INITIAL DEPLOYMENT SITE (FOL/FOB)**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
	F. Have you made contact with the Threat Working Group members? (1) Have you scheduled TWG meetings? (2) Have you set force protection information sharing procedures? (3) Have you, in coordination with the TWG, completed the Force Protection EEI checklist and transmitted it in the form of an INTREP to HQ *AMC/INO*? G. Send OSTREP IAW AMCI 14-102. 2. Living accommodations: A. Do intelligence personnel have adequate quarters? B. Do intelligence personnel have dining arrangements? 3. Work-schedule: Have you established work shifts and sent non-essential personnel to their quarters to rest? 4. Work-area set up: A. Have you unloaded supplies/equipment from the pallet? B. Have you started tracking missions? C. Have you started an events log? D. Have you posted charts with the situation and latest OB?			

	E. Are supplies/equipment and forms/documents ready for use? F. Have you established a briefing schedule? 5. Message traffic: A. Is all message traffic arriving in a timely manner? B. Have you established a message log? C. Are messages initialed after reading/posting and posted with a log number?			

CHECKLIST		PAGE 3 OF 3 PAGES		
TITLE/SUBJECT/ACTIVITY **INITIAL DEPLOYMENT SITE (FOL/FOB)**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
	6. GI&S: A. Do you continually update the OB/situation board? B. Does the chart have proper classification markings and "Current as of" time? C. Does the chart have a clear legend? 7. Analysis, interpretation, and evaluation: A. Is all information evaluated for: (1) How it affects the mission? (2) How it affects the aircrews? (3) How it affects the base? B. Who requires information (Wing/CC, CAT, Tactics, TWG, etc.)? C. Have your interpreted the information? How does it affect enemy and friendly actions? Do you have any recommendations?			

CHECKLIST		PAGE 1 OF 1 PAGES		
TITLE/SUBJECT/ACTIVITY **INTEL RE-DEPLOYMENT**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
	1. Inventory all classified materials on hand using AF FORM 310. 2. Affix "Materials Exempt from Examination" statement to the outside of all IN's classified containers. 3. Inventory the equipment on hand using the IN Mobility Equipment listing to account for all equipment. 4. Securely pack all deployment equipment to ensure safe arrival at home station. 5. Place one copy of the IN Mobility Equipment list on the inside of the bin, and a second, sealed copy, on the outside of the bin. 6. Ensure all Intel personnel are on a chalk and will arrive in time to re-deploy.			

CHECKLIST		PAGE 1 OF 1 PAGES		
TITLE/SUBJECT/ACTIVITY **INTEL EVACUATION**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
	Note: *Be prepared at all times for a possible evacuation. Keep all classified in a central location, work out of bug-out boxes/bags, and have evacuation items ready to go at a moment's notice. Identify and post the responsibilities of each individual and know where to relocate.* When notified: 1. Assemble and inventory all classified materials. A. Gather required classified material for evacuation. (1) Situation maps. (2) Vital library documents. (3) Read files. (4) Message traffic. (5) Laptop Computer, disks, and printer. (6) STU-III/fax/key. (7) All COMSEC. (8) ISOPREPs. B. Lock material not required for evacuation in safe, or if required, destroy material. (1) Inventory all classified identified for destruction.			

	(2) Destroy at central destruction facility or by shredding/burning by unit personnel. C. Check area for classified left behind. D. Account for all personnel. E. Take all personal gear and bug-out boxes/bags and evacuate the area. 2. At relocation area: A. Account for all personnel. B. Account for all classified material. C. Notify appropriate local agencies of relocation and provide new phone numbers. D. File OSTREP to notify HHQ of new location and phone numbers.			

CHECKLIST		PAGE 1 OF 1 PAGES		
TITLE/SUBJECT/ACTIVITY **POST DEPLOYMENT**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
	1. Take the following steps to prepare mobility assets future tasking. A. Supplies: (1) Count all supplies and compile a shortage list; order necessary items. (2) Repack supplies correctly in their respective boxes. (3) Properly seal and label the mobility boxes. B. Equipment: (1) Check each piece of equipment to ensure it works. (2) Identify equipment shortages; notify equipment custodian of any damaged or missing equipment. (3) Repack equipment correctly in the proper mobility bin. C. Forms: (1) Count all forms and compile a shortage list; order necessary forms. (2) Repack forms correctly into their respective boxes. 2. Correctly label all mobility boxes and prepare IN mobility assets for the next mobility tasking.			

SAMPLE OPERATING INSTRUCTION

1. GENERAL: This OI identifies responsibilities and procedures for preparation and deployment of intelligence personnel and equipment assigned to the *(your unit)*.

2. PURPOSE: The purpose of this OI is to ensure the smooth and efficient transition of personnel, equipment, supplies, materials and publications from garrison to the deployed forward location during exercise and real world contingencies.

3. DIRECTIVES: This is an optional OI recommended in AMCPAM 14-103, *Procedures for Requesting Intelligence Information and Imagery*.

4. REFERENCES:

A. Applicable OPLANs.

B. AFI 10-403, *Deployment Planning*.

C. AFI 31-401, *Managing the Information Security Program*.

D. AMC supplement to AFI 14-105, *Unit Intelligence Management*.

E. AMCPAM 14-104, *Intelligence Handbook*.

5. RESPONSIBILITIES:

A. The Intelligence Flight Commander is responsible for the following:

(1) Overall management of the unit's mobility program.

(2) Appointing a Unit Deployment Manager (UDM) to ensure effective management of the mobility program.

(3) Developing and ensuring periodic maintenance of the mobility OI.

B. The UDM is responsible for the following:

(1) Day-to-day management of the mobility program.

(2) Ensuring the accuracy and currency of the checklists both within this OI and those used for contingencies.

(3) Tracking and scheduling necessary training to maintain currency for mobility (coordinate with Wing Mobility Manager).

(4) Standardizing unit mobility folders and ensuring their currency. The Wing Mobility Manager will ensure overall standardization.

(5) Updating the mobility OI as necessary.

(6) Monitor current levy flow from Wing XP and ensure name(s) are assigned to each levy against the unit.

Each individual is responsible for being familiar with this OI, carrying out its provisions, and for identifying deficiencies, errors, or omissions. This includes individual responsibility for ensuring currency for their own training and mobility folders.

6. PREREQUISITES: Newly assigned personnel will complete the following actions ASAP:

A. Attend Chemical Warfare Training (initial or refresher, as applicable).

B. Attend Self-Aid Buddy Care (initial or refresher, as applicable).

C. Attend Law of Armed Conflict Briefing.

D. Attend Explosive Ordnance Training.

E. Obtain an Official U.S. Passport (military as a minimum, preferably a civilian one).

F. Process through the Immunization Clinic.

G. Qualify on 9mm/M-9.

H. Maintain personal items, finances, and dependent care in a state, which will allow for short notice deployment (see Atch 1 for individual responsibilities).

7. GENERAL PROCEDURES: When notified of a recall, all section personnel will report to their duty sections IAW alerting instructions. Review and supplement mobility procedures outlined in this mobility book and the Intelligence Deployment Operations Book (one issued to each individual).

8. EQUIPMENT PROCEDURES:

A. The mobility OPR will inventory, pack, and palletize mobility equipment, supplies and documents.

B. The Logistics Detail (LOGDET) of UTC PFMA7/PFMAG/PFMAH lists the standard equipment. This list will include the item National Stock Number (NSN), item nomenclature (noun), quantity, Table of Allowance (TA) and quantity to be on stock.

C. Attach 2 lists equipment required for deployment. Modify the list to suit the needs of the deployment.

9. SUPPLY PROCEDURES:

A. Prepackage mobility supplies into mobility boxes; however, a final check of the boxes is necessary to ensure a 30-day supply of all major items is available. Listed on the inside of each box is an annual inventory; additionally, the Intelligence Mobility OPR maintains a copy.

B. At this time, determine if you need other supply items not already identified for mobility.

C. See Atch 2 for complete list of supplies.

10. PUBLICATION PROCEDURES:

A. Attachment 3 is a list of documents identified for deployment.

B. Place all unclassified documents in a separate mobility box.

C. Place classified documents in appropriately secure containers for transport. This could include securing classified documents in the mobility safe or hand-carried by official couriers. Mark the containers with the placard **"OFFICIAL BUSINESS, MATERIAL EXEMPT FROM EXAMINATION"** (Atch 6), signed by the authorizing official who signed the courier letter, (Atch 4). Give a listing of classified documents for each container to the mobility OPR and place one in the respective container.

D. Have AF Form 12, *Accountable Container Receipt*, for the containers on hand prior to each deployment. The classified couriers will retain the AF Form 12 as a receipt, should it become necessary to store classified at a base other than the final destination.

E. Identify all intelligence personnel as classified couriers. Each is responsible for the safeguarding of classified material until it reaches its destination. Their orders will designate them, as couriers for classified materials and one copy of their orders, along with a copy of their courier letter, will remain with the home unit POC.

11. GI&S Procedures: Specific GI&S requirements are found in Annex M of the applicable OPLAN. The GI&S monitor will designate charts for each mobility requirement.

JOHN A. DOE, Capt, USAF
Commander, Intelligence Flight

Attachments:
1. Personal Mobility Preparation
2. Mobility Equipment Inventory Checklist
3. Deployment Documents Checklist
4. Designation of Official Courier Letter
5. Authorization to Pick-up Message Traffic Letter
6. Classified Container Cover Letter

Attachment 1

Personal Mobility Preparation

1. Personnel will ensure all items listed below are current and up-to-date to alleviate accomplishing them in the mobility processing line (see unit Mobility Officer or NCO for a complete listing).

A. Immunization certificate (shot records)

B. Metal ID tags (dog tags)

C. Military ID card

D. Restricted Area Badge (line badge)

E. Current Leave and Earnings Statement

F. Official Passport

G. Government credit card

H. DD Form 93, Record of Emergency Data

I. Required military clothing (See Tab A)

J. Minimum essential civilian clothing and personal items (See Tab B)

K. Gas mask glasses insert (if applicable)

L. On-The-Job (OJT) training records for E-6 and below

M. Weapons Qualification card(s)

N. All required training accomplished (LOAC, Force Protection, SABC, etc)

O. 30-day supply of medication if you are under medical care. Advise medical personnel in the mobility line if you are receiving medical treatment or have a chronic medical problem so your medical records can be reviewed.

P. Legal responsibilities (Power(s) of Attorney, Dependent Care Plan, Will, SGLI)

Q. Cancel all appointments (Doctor, Dentist, Quality, etc.)

2. Prior to deployment, mobility assigned personnel will familiarize themselves with procedures and operations they can expect to encounter at the Forward Operating Location (FOL.)

TAB A to Attachment 1

Military Clothing Requirements

1. Required items to take on a standard deployment:

A. 1 A-3 Kit bag (canvas bag, supplied by unit)

B. 1 Belt, w/black clip and buckle

C. 1 pair Combat boots

D. 1 BDU/DCU utility cap (baseball caps not authorized for deployment) w/subdued rank

E. 4 sets BDUs/DCUs with proper insignia (subdued rank)

F. 7 sets of undergarments (T-shirts/Underwear/Bras)

G. 7 pairs of socks (black)

H. 1 BDU/DCU field jacket

I. 1 pair gloves w/inserts

J. Extra pair eyeglasses (if needed)

K. Civilian Clothes (See Tab B)

L. Toilet Kit (See Tab B)

M. Reflective belt

N. Medication, if required (enough to last duration of deployment)

O. Work gloves

2. Mobility Bags (See your Unit Deployment Manager (UDM) for A-Bag, B-Bag and C-Bag listing)

A. A Bag: General purpose bag.

B. B Bag: Cold Weather bag

C. C Bag: Four complete chemical warfare defense ensembles (CWDE).

1) Mini C Bag: Minimum CWDE to survive a chemical attack (Mask and one GCE)

2) ATSO Training C Bag: Real world mask and training GCE for use during base/wing exercises.

D. D Bag: CWDE individual Aircrew Ensemble

E. E Bag: Desert gear

TAB B to Attachment 1

Minimum Essential Civilian Clothing and Personal Items

1. Civilian clothes:

A. At least one set for sightseeing or visiting local officials' homes. Remember, you want to blend in with the local population; dress accordingly.

B. Shower gear (what you think necessary to trek to outdoor shower facilities), including robe, shoes, and shower thongs.

C. Extra pairs of contact lenses, solution, and enzymes, if applicable.

2. Toilet Kit: Recommend purchase of toilet kit and incidentals at home station because of ration restrictions and saturation of deployment base facilities during exercises. Recommend the basic toilet and personal hygiene kit include the following:

Core Items	Unit	30-Day	60-Day
Deodorant (stick)	Ea	1	2
Soap (3½-4 oz bar)	Bar	2	4
Shampoo	Tube	2	4

Toothbrush w/container	Ea	1	1
Toothpaste	Tube	1	2
Comb/Brush	Ea	1	1
Towel	Ea	2	3
Washcloth	Ea	2	3
Nail Clipper	Ea	1	1
Male			
Shaving Cream (Pressurized)	Can	1	2
Razor (disposable)	Pkg	3	5
Female			
Lotion (hand/body)	Tube	1	2
Napkin/sanitary, self-adhesive	Box	1	2
Tampon, sanitary	Pkg	1	2
Tissue	Box	1	1

3. Use the following list of personal comfort items as a guide only--baggage weight and size restrictions will limit what can be brought:

A. Battery/spring operated alarm clock

B. Flashlight w/extra batteries

C. Books or other off-duty entertainment, such as Game Boy® systems, Cards, etc.

D. Sunglasses

E. Medical Kit, containing: aspirin, antacid, Sudafed, band-aids, anti-diuretics, prescription drugs, etc.

F. Padlocks

G. Watch (leave expensive jewelry at home)

H. Cash and personal/travelers checks

I. Officer/NCO Club card

J. Handkerchiefs

K. Can opener

L. Sewing kit

M. Pocket knife

N. Matches or lighter

O. Pens/pencils/paper/envelopes/stamps/address book

P. Spare shoe/boot laces

Q. Laundry bag

R. Laundry detergent

S. Shoe polish

T. Extra shoes/Boots

U. Make-up kit

4. If deploying under field conditions, consider bringing:

A. Toilet paper

B. Foot powder.

C. Insect repellent

D. Sunscreen

E. Air mattress and pillow

F. 10-20 feet of rope

G. Mosquito netting (summer)

H. Small ice chest

I. Portable radio w/cassette or CD player

Attachment 2

Mobility Equipment Inventory Checklist

(PFMAH)

Container Number	Item Description	Location
Palletized Items		
Administrative supplies (Tab A)		
001A	Field Desk #1 Mobility/Supply room	
General Deployment	Equipment (Tab B)	
002A	2 Dr Safe #1	Mobility/Supply room
003A	Equipment Can #1 (Large green can)	Mobility/Supply room
004A	Equipment Can #2 (Large green can)	Mobility/Supply room
005A	Equipment Can #3 (Large green can)	Mobility/Supply room
006A	Metal Dolly #1	Mobility/Supply room
007A	Metal Roller #1	Mobility/Supply room
008A	Shredder	IN Vault
009A-014A	Folding Chairs	Mobility/Supply room
015A-018A	Folding Tables	Mobility/Supply room
019A	Monitor, 20in	Mobility/Supply room
Hand-carry Items (Tab C)		
020A	CMF Case #1 (COMSEC)	Mobility/Supply room
021A	CMF Case #2	Mobility/Supply room
022A	Map Tube #1	Mobility/Supply room

TAB A to Attachment 2

Administrative Supplies

Field Desk #1 (Mobility Container *(your unit)* #001A)

Item	Unit	Quantity
Acetate Sheets		
Clear, Overhead	Box	2
Stickyback	Box	2
Batteries (proper size for clocks, flashlights, radios)	Pack	2
Briefing in Progress Sign	Ea	2
Chart Pak (various kinds)	Ea	As Determined
Classified Waste Bags (plastic/paper)	Ea	5
Clock	Ea	1
Colored Markers		
- Red, Blue, Black, Green		
-- Fine, Water Soluble	Ea	10
-- Medium, Water Soluble	Ea	10
-- Large, Permanent	Ea	4
- Orange, Yellow, Purple		
-- Fine, Water Soluble	Ea	5
-- Medium, Water Soluble	Ea	3
-- Large, Permanent	Ea	2
- Highlighters	Set	1
- Dry Erase Markers	Set	1
Clipboards	Ea	5
Computer Supplies		
- Disks		
--3½" (High Density)	Box	2
-- CD Rom Disks (RW)	Box	2
-- Labels		
--- Secret	Sheets	5
--- Confidential	Sheets	5
--- Unclassified	Sheets	5
Dividers	Set	2
Document carrier	Ea	2
Envelopes		
- Large, Brown (8½x11)	Ea	20
- White, Letter	Ea	15
Flashlight w/batteries	Ea	2

Folder		
- Blue, two pocket	Ea	5
- Brown, 6 Section	Ea	10
Forms (Blank)		
- DD Form 1833 Isolated Personnel Report (blank)	Ea	15
- AF Form 310 Document Receipt & Destruction Cert.	Ea	10
- AF Form 614 Charge Out Record	Ea	10
- SF Form 701 Activity Security Checklist	Ea	5
- SF Form 702 Secret Container Checklist	Ea	6
- SF Form 704 Secret Cover Sheet	Ea	25
- SF Form 705 Confidential Cover Sheet	Ea	10
- AF Form 12, Sign-out Receipt Form	Ea	10
Intelligence Deployment Operations Checklist	Ea	ind. copy
Large Coffee Can (Emergency Destruction)	Ea	1
Leatherman Tool	Ea	1
Logbook	Ea	1
Notebook		
- Spiral, Small	Ea	2
- Letter, White	Ea	3
- Legal, Yellow	Ea	3
Note Pads, Post It		
-2"x 2"	Box	1
- 3"x 5"	Box	1
Order of Battle Symbols (Red Black Blue)		
-Aircraft	Box	2
- EW/GCI	Box	2
- Missile, large	Box	2
- Missile, small	Box	1
- Naval (large ship)	Box	2
Paper Clips	Box	2
Pencil Erasers	Box	1
Pencils	Box	2
Pencil Sharpener	Ea	1

Pens, Black	Box	2
Plastic overlay	Roll	1
Plotter, Weems	Ea	2
Razor Blades	Box	1
Scissors	Ea	2
Screwdriver Set	Ea	1
Security		
- Stamps		
-- Secret	Ea	2
-- Unclassified	Ea	2
-- This page blank	Ea	2
	Ea	2
- Ink Pad	Ea	2
Staple Remover	Ea	2
Stapler	Ea	1
Staples	Box	2
Straight Edge		
- Large (18")	Ea	2
- Small (12")	Ea	2
Tape		
- Dispenser	Ea	1
- Duct (Red, Black)	Roll	3
- Masking	Roll	2
- Scotch	Roll	5
Template (Holometer)	Ea	4
Template, UTM	Ea	2
Tissue	Box	2
Three Hole Punch	Ea	1
Thumb Tacks	Box	2
Two Hole Punch	Ea	1

TAB B to Attachment 2

General Deployment Equipment

2 Drawer Safe #1 (Mobility Container *(your unit)* #002A)

Shipped empty as Standard Operating Procedure.

Can ship classified if coordinated through Wing Mobility Manager.

Equipment Can #1 (Mobility Container *(your unit)* #003A)
Acetate, Stickyback.
STU-III-Fax w/ applicable cables and cords.
AC/DC Light.
Short Wave Radio.
Equipment Can #2 (Mobility Container *(your unit)* #004A)
2 X Surge Protectors.
Projector, Overhead.
Laptop w/ printer and all applicable cables and cords.
Backup disks.
25' Extension Cord.
Equipment Can #3 (Mobility Container *(your unit)* #005A)
Black and White Copier.
Video Projection System.
Transformer.
Metal Dolly #1 (Mobility Container *(your unit)* #006A)

Shredder (Mobility Container *(your unit)* #008A)

Folding Chairs (Mobility Containers *(your unit)* #009A-014A)

Folding Tables (Mobility Containers *(your unit)* #015A-018A)

Monitor, 20in (Mobility Container *(your unit)* #019A)
TAB C to Attachment 2

Hand-Carried Items

CMF Case #1 (Mobility Container *(your unit)* #034A)
Hand carried Classified Items (COMSEC).
CMF Case #2 (Mobility Container *(your unit)* #035A)
Hand carried Classified Items.
Map Tube #1 (Mobility Container *(your unit)* #036A)
Attachment 3

Deployment Documents Checklist (Ref. AMC supplement to AFI 14-105)

This listing is a guide only. These documents are the most important in our inventory. The type and quantity of document will depend on the deployment location. Check with the lead unit at the deployment location or HQ AMC for document requirements (if applicable).

1. Core Items:
   - A. The World Fact Book (CPAS-WF-YR-002).
   - B. The World Fact Book, Classified Supplement (CPAS-WF-YR-002).
   - C. Annual Reevaluation of SAFEs (ARSA) - (OGA-2100-48-92 CRDL:05401).
   - D. NIMA Catalog of Maps, Charts and Related Products
   - E. Joint Pub 3-50.2, Joint Doctrine for Evasion and Recovery.
   - F. Joint Pub 3-50.3, Doctrine for Joint Combat Search and Rescue.
   - G. AFTTP 3-1, Vol. 1 & Vol. 2
   - H AFI 14-105, Unit Intelligence Mission and Responsibilities.
   - I. AMC supplement to AFI 14-105
   - J. AMCI 14-102, Debriefing and Reporting.
   - K. AMCP 14-104, AMC Intelligence Handbook.
   - L. AMCP 14-103, Procedures for Requesting Intelligence Information and Imagery.
   - M. Intelligence Deployment Operations Book.
   - N. Jane's All the World Aircraft (most current edition at a minimum).
   - O. Jane's All the World Ships (most current edition at a minimum).
   - P. World Atlas.
   - Q. Dictionary.
   - R. Thesaurus.
   - S. Home station phone book and AMC directory.
   - T. Tongue and Quill.
2. Area Specific:
   - A. Recognition Guides
   - B. Fin flash graphic for region.
   - C. Selected Area for Evasion (SAFE)/Safe Area Intelligence Descriptions (SAID)
   - D. DIA Military Capabilities Studies (MCS) - (DDB-2680-XX-YR).
   - E. SERE Contingency Reference Guides (USAFINTEL 400 Series).
   - F . Maps and Charts for region.
3. Unit Specific:
   - A . Geopolitical studies/capabilities.
   - B . Prepackaged threat briefings.

Attachment 4

Designation of Official Courier Letter (Example)

Must Be On Letterhead Stationery

MEMORANDUM FOR WHOM IT MAY CONCERN (Date)

FROM: Unit
Street Address
Base, State, Zip

SUBJECT: Official Courier of Classified Information

1. (Rank, Name, SSAN, unit, base, state, zip) is an official courier for the United States Government. Upon request, he will present his official identification card bearing the number (ID card Number).

2. (Rank, Surname) is hand carrying a (description of the package to include size), addressed to (gaining unit). It is identified on the outside of the package by the marking "**OFFICIAL BUSINESS, MATERIAL EXEMPT FROM EXAMINATION**" and bearing the signature of the undersigned.

3. (Rank, Surname) is departing (departure point) with a final destination of (destination). He has transfer points at (list all transfer points).

4. You can confirm this courier designation by contacting the undersigned at Comm: (xxx) xxx-xxxx, DSN: xxx-xxxx. This letter expires (Date).

Signature Block

Attachment 5
Authorization to Pick Up Message Traffic Letter
MEMORANDUM FOR WHOM IT MAY CONCERN (Date)
FROM: UNIT
SUBJECT: Authorization to pick up message traffic

1. The following individuals are authorized to pick up message traffic. The local security manager verified all clearance information.
2. Name Social Security NumberID NumberClearance
3. Direct any questions to the Senior Intelligence Officer/NCO, (rank, name and phone) or the Unit Security Manager, (rank, name and phone).
(Signature Block of Appropriate Authority usually SIO or Security Manager)
Attachment 6
Classified Container Cover Letter (Example)
DEPARTMENT OF THE AIR FORCE
(YOUR UNIT)
(YOUR UNIT ADDRESS)
_____
Official Business
_____
MATERIAL EXEMPT FROM EXAMINATION

(Signature Block of Appropriate Authority)
(Must match signature of Courier Letter)

Chapter 13

OPLAN 8044 (SIOP)

13.1. General. The SIOP is the "blueprint" for the implementation of the Emergency War Order to conduct long range strikes against designated targets. The role of the tankers is crucial to obtain "GLOBAL ENGAGEMENT."

13.2. Reference Documents (Classified documents)

- OPLAN 8044-96
- COMAMC 8044-FY
- AMCI 10-450V1, *KC-135 SIOP Generation/Expanded Alert*
- AMCI 10-450V2, *KC-135 SIOP Planning*
- AMCI 10-450V4, *Support of Alert Forces*

13.3. SIOP Planning. The Joint Chiefs of Staff (JCS) chart series satisfies AMC requirements for Combat Mission Folder construction and operational staff planning in support of SIOP forces. These classified charts are standard charts overprinted with special navigation and defensive OB information, vital to aircrews in the execution of the SIOP.

13.3.1. Assumption of Alert (AOA). Initial aircrew briefing upon declaration of an alert hour (A-hour) in order to assume sortie responsibility. Background brief and pre-mission brief rolled into one. Generation of aircraft to SIOP status is paramount – if crews are not available for the briefing due to aircraft generation, a handout containing critical briefing items will be given to crews enroute to aircraft. (Ref AMCI 10-450V1/V4)

13.3.2. Combat Mission Folders (CMF). The CMF is an all-encompassing product comprised of many parts that gives direction and purpose for aircrew. The minimum intelligence contribution to the CMF should include imagery/information on post-strike/recovery bases and all relevant route threat data (leg-by-leg and a mission overview, as applicable). (Ref AMCI 10-450V2)

13.3.3. Unit Mission Brief (UMB). The UMB is an overview of all the unit's entire SIOP taskings, including information common to all sorties. It presents an overview of mission routing, concepts, and the general threat scenario – the "big picture." Don't forget to include information about recovery, divert, abort, and alternate airfields, as well as future weapon developments that may have an impact later.

13.3.4. Initial Sortie Study (ISS). The ISS is a booklet that contains more detailed, mission specific information that the aircrew can check out for study. It should review potential threat and enemy defense capabilities to include air, ground, and naval threats. Be sure to make note of active and passive EW/GCI and IFF lines.

13.3.5. Aircrew Certification Training. Intelligence units provide CoCCT and threat training as part of the aircrew certification training process. (Ref AMCI 10-450V4)

CHECKLIST		PAGE 1 OF 2 PAGES		
TITLE/SUBJECT/ACTIVITY **OPLAN 8044 GENERATION CHECKLIST**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
1	Assumption of Alert (AOA) Briefing (bring all crew ISOPREPcards) a. Secure the room (radios/bricks/telephones, doors/windows, guards posted, clearances verified) b. Security classification c. Information "current as of" time d. Brief summary of events leading to AOA e. General political situation f. Military situation, to include status of ICBM, air, naval (including AGIs), and conventional forces g. Estimate of enemy intentions (24-48 hrs) h. Route threat information i. Recovery/divert/abort alternate airfields j. Evasion and recovery info - SAFEs/SAIDs - Sanitization reminder - Distribute E&R kits (have crews sign for kits) - ISOPREP review reminder - Create/review/update EPAs k. Debriefing and reporting instructions to include INFLTREP, MISREP, AFSIR (formerly MIJI), debriefing location and POC, EEI reminder l. Local threat/Satellite over-flight times m OPSEC/COMSEC reminder			

CHECKLIST		PAGE 2 OF 2 PAGES		
TITLE/SUBJECT/ACTIVITY **OPLAN 8044 GENERATION CHECKLIST**		OPR	DATE	
NO.	ITEM *(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph.)*	YES	NO	N/A
	n. Solicit Questions o. Security classification and "current as of" time reminder			
2	Complete ISOPREP review/update for all alert crews			
3	Issue Combat Mission Folder (CMF) Containers/sortie cans			
	a. Ask aircrew sortie number			
	b. Remove corresponding CMF container from storage area			
	c. Have aircrew page count all material in CMF			
	d. Have crewmember date and sign CMF tracking worksheet			
4	Assist crews in CMF study/Individual Sortie Study (ISS) as required			
5	CAT briefing (ref CAT/BS Briefing checklist) Conduct follow-on AOA and CAT briefings as required (aircrews and CAT should be briefed on developments that may affect posture changes, local security, or threats to aircraft)			
6	Return of CMF containers/sortie cans			
	a. Verify CMF contents by performing page count of all materials			
7	b. Sign CMF tracking worksheet			
	c. Return CMF to storage area			

STEVEN R. CAPENOS, Colonel, USAF
Director of Intelligence

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoD-0000-151A-95, *Department Of Defense Intelligence Production Program: Production Responsibilies*

DoD 1300.7, *DoD Training And Education Measures Necessary To Support The Code Of Conduct*

DoD 2310.2*DoD Personnel Recovery*

DoD 5200.1-PH, *DoD Guide To Marking Classified Documents*

DoD 5200.1R, *DoD Information Security Program*

DoD 5200.2R, *DoD Personnel Security Program*

JOINT PUB 3-50.2, *DOCTRINE FOR JOINT COMBAT SEARCH AND RESCUE*

JP 3-50.3, *Joint Doctrine For Evasion And Recovery*

JP 3-50.21, *Joint Tactics, Techniques, And Procedures For Combat Search And Rescue*

AFDD 1-1, *Air Force Task List*

AFDD 2-1.6, *Combat Search And Rescue*

AFI 10-403, *Deployment Planning*

AFI 11-301, *Aircrew Life Support*

AFI 14-103, *Procedures For Requesting Intelligence Information And Imagery*

AFI 14-104, *Oversight Of Intelligence Activities*

AFI 14-105, *Unit Intelligence Mission And Responsibilities* (Also see AFI 14-105 AMC1)

AFPAM 14-118, *Aerospace Intelligence Preparation Of The Battlespace*

AFI 14-201, *Intelligence Production And Application*

AFI 14-205, *Identifying Requirements For Obtaining And Using Cartographic And Geodetic Products And Services*

AFI 16-1301, *Survival, Evasion, Resistance, And Escape Program*

AFI 16-107, *International Personnel Exchange Program (PEP)* (also see AFI 16-107 AMC1)

AFI 16-201, *Disclosure Of Military Information To Foreign Governments And International Organizations*

AFI 16-1301, *Survival, Evasion, Resistance, And Escape (SERE) Operations And Training*

AFI 31-401, *Information Security Program Management*

AFI 31-406, *Applying The North Atlantic Treaty Organization (NATO) Protection Standards*

AFI 31-501, *Personnel Security Program Management*

AFI 33-202, *Computer Security*

AFI 33-203, *Emission Security*

AFI 33-209, *Operational Instruction For The Secure Telephone Unit (STU-III) Type 1*

AFI 33-211, *Communications Security (COMSEC) User Requirements*

AFI 33-212, *Reporting Comsec Deviations*

AFI 36-2108, *Airman Classification*

AFI 36-2201, *Developing, Managing, And Conducting Training*

AFMAN 36-2247, *Planning, Conducting, Administering, And Evaluating Training*

AFI 36-2847, *Intelligence Awards*

AFI 36-8002, *Telecommuting Guidelines For Air Force And Their Supervisors*

AFMAN 37-123, *Management Of Orders*

AFI 90-201, *Inspector General Activities*

CJCSI 3270.01, *Personnel Recovery Within The Department Of Defense*

FM 101-5-1, *Operational Terms And Graphics*

FM 34-130, *Intelligence Preparation Of The Battlefield*

AMCI 10-450V1, *(S) KC-135 SIOP Generation/Expanded Alert (U)*

AMCI 10-450V2, *(S) KC-135 SIOP Planning (U)*

AMCI 10-450V4, *(S) Support Of Alert Forces (U)*

AMCI 14-102, *Intelligence Debriefing And Reporting*

AMCI 14-107, *Command Intelligence Personnel Training Program*

AMCI 90-201, *The Inspection System*

AMCP90-202, *Operational Readiness Inspection Guide*

HOI 36-2803, *Support For Higher Headquarters Gatekeeper Program*

MIL-STD-2525B, *Department Of Defense Interface Standard-Common Warfighting Symbology*

Abbreviations and Acronyms

AAA —Antiaircraft Artillery

AAAOB —Antiaircraft Order-of-Battle

AAFIF —Automated Air Facilities Information File

ABCCC —Airborne Battlefield Command and Control Center

ACO —Airspace Coordination Order

ADPE —Automated Data Processing Equipment

ADS —Active Duty Support

ADT —Active Duty for Training

AETC —Air Education and Training Command

AFCC —Air Force Component Commander

AFDD —Air Force Doctrine Document

AFI —Air Force Instruction

AFPAM —Air Force Pamphlet

AFPD —Air Force Policy Directive

AFRES —Air Force Reserve

AFSC —Air Force Specialty Code

AFSOC —Air Force Special Operations Command

AFTL —Air Force Task List

AGI —Auxillery Intelligence Gathering (Naval Vessel)

AI —Area of Interest

AIS —Automated Information System

AIT —Aircrew Intelligence Training

AMCIT —American Citizen

AMD —Air Mobility Division

AMOS —Air Mobility Operations Squadron

AMT —Air Mobility Tasking

AMWC —Air Mobility Warfare Center

AOA —Assumption of Alert

AOB —Air Order-of-Battle

AOC —Air Operations Center

AOR —Area of Responsibility

ARC —Air Reserve Component

AT —Annual Training

ATO —Air Tasking Order

ATSO —Ability to Survive and Operate

AUTODIN —Automatic Digital Network

AWACS —Airborne Warning and Control System

BS —Battle Staff

C2 —Command and Control

CAF —Combat Air Forces

CAT —Crisis Action Team

CC —Commander

CD-ROM —Compact Disc Read Only Memory

CDM —Command Dissemination Manager

CDRG —Compressed Digitized Raster Graphics

CENTCOM —Central Command

CFETP —Career Field Education and Training Plan

CHOP —Change Operational Control

CIB —Controlled Image Base; Current Intelligence Briefing

CJCS —Chairman, Joint Chiefs of Staff

CMF —Combat Mission Folder

COA —Course of Action

CoC —Code of Conduct

CoCT —Code of Conduct Training

CoCCT —Code of Conduct Continuation Training

COG —Centers of Gravity

COMACC —Commander Air Combat Command

COMAMC —Commander Air Mobility Command

COMPUSEC —Computer Security

COMSEC —Communication Security

CONPLAN —Contingency Plan

CONUS —Continental United States

COTS —Commercial Off-the-Shelf

CP —Command Post

CRRS —Customer Requirements Registration System

CSAR —Combat Search and Rescue

CSI —Contingency SERE Indoctrination

CSSO —Computer Systems Security Officer

DDA —Designated Disclosure Authority

DDL —Delegation of Disclosure Authority Letter

DF —Direction Finding

DIA —Defense Intelligence Agency

DIRMOBFOR —Director of Mobility Forces

DISA —Defense Information System Agency

DISK —Deployable Intelligence Support Kit

DMD —Deployment Manning Document

DMOB —Defensive Missile Order-of-Battle

DMS —Defense Message System

DOC —Designed Operational Capability

DOD —Department of Defense

DPM —Dissemination Program Manager

DTED —Digital Terrain Elevation Data

E&E —Evasion and Escape

E&R —Evasion and Recovery

E&R/CSAR —Evasion and Recovery/Combat Search and Rescue

EAF —Expeditionary Aerospace Force

ECI —Extension Course Institute

EEI —Essential Elements of Information

EOB —Electronic Order-of-Battle

EOC —End-of-Course

EORI —Expeditionary Operational Readiness Inspection

EPA —Evasion Plan of Action

ERO —Engine Running On-Loads/Off-Loads

EUCOM —European Command

EVC —Evasion Chart

FDO —Foreign Disclosure Officer

FEBA —Forward Edge of the Battle Area

FLOT —Forward Line-of-Own Troops

FM —Field Manual; Financial Manager

FOB —Forward Operating Base

FOL —Forward Operating Location

FP —Force Protection

FSCL —Fire Support Coordination Line

FY —Fiscal Year

GCI —Ground Control Intercept

GI&S —Geospatial Information & Services

GOB —Ground Order-of-Battle

GOTS —Government Off-the-Shelf

GPS —Global Positioning System

GSA —Government Services Administration

HHQ —Higher Headquarters

HQ —Headquarters

HUMINT —Human Resources Intelligence

HVAA —High Value Airborne Asset

IADS —Integrated Air Defense System

IAW —In Accordance With

ICE —Intelligence Collaborative Environment

IDT —Inactive Duty Training

IG —Inspector General

IIS —Intelligence Information Systems

IMA —Individual Mobilization Augmentee

IN —Intelligence; Intelligence Flight Commander

INFLTREP —In-Flight Report

INFOSEC —Information Security

INMARSAT —International Maritime Satellite System

INTEL —Intelligence

INTELINK —An integrated intelligence dissemination and collaboration service at the Sensitive Compartmented Information classification level.

INTELINK-S —An integrated intelligence dissemination and collaboration service at the SECRET classification level.

INTL —Intelligence Task List

INTREP —Intelligence Report

INTSUM —Intelligence Summary

IPB —Intelligence Preparation of the Battlespace

IR —Initial Response

ISOPREP —Isolated Personnel Report

ISP —Internet Service Provider

ISPM —Information Security Program Manager

ISS —Initial Sortie Study

JA/ATT —Joint Airborne/Air Transportability Training

JAC —Joint Analysis Center

JCAVS —Joint Clearance Access Verification System

JCS —Joint Chiefs of Staff

JDS —Joint Dissemination System

JIC —Joint Intelligence Center

JFC —Joint Forces Commander

JOPES —Joint Operations Planning Execution System

JP —Joint Publication

JPRA —Joint Personnel Recovery Agency

JQS —Job Qualification Standard

JRCC —Joint Rescue Coordination Center

JSRC —Joint Search and Rescue Center

JWICS —Joint Worldwide Intelligence Communication System

LAN —Local Area Network

LOAC —Law of Armed Conflict

LZ —Landing Zone

M&M —Manpower and Material

MAJCOM —Major Command

MCS —Military Capabilities Study

MDS —Mission Design Series

MET —Management Engineering Team

METL —Mission Essential Task List

MIA —Missing in Action

MIDB —Modernized Intelligence Data System

MIJI —Meaconing, Intrusion, Jamming, and Interference

MISREP —Mission Report

MOB —Missile Order of Battle

MOPP —Mission Oriented Protective Posture

MPA —Military Personnel Appropriation

MPF —Military Personnel Flight

MRR —Minimum Risk Routing

MTT —Mobile Training Teams

NAF —Numbered Air Force

NATO —North Atlantic Treaty Organization

NBC —Nuclear, Biological, Chemical

NIMA —National Imagery and Mapping Agency

NM —Nautical Mile

NOB —Naval Order-of-Battle

NRT —Near-Real-Time

OA —Operational Area

OB —Order-of-Battle

OFFREP —Off-Station Report

OI —Operating Instruction

OIC —Officer-in-Charge

OJT —On-the-Job Training

OPCON —Operational Control

OPLAN —Operations Plan

OPORD —Operation Order

OPR —Office of Primary Responsibility

OPSEC —Operations Security

ORI —Operational Readiness Inspection

OSI —Office of Special Investigations

OSS —Operation Support Squadron

OSTREP —On-Station Report

PACAF —Pacific Air Forces

PACOM —Pacific Command

PBA —Predictive Battlespace Awareness

PC —Personal Computer

PC-13 —Personnel Computer Integrated Imagery and Intelligence

PCS —Permanent Change of Station

PFPS —Portable Flight Planning Software

PLA —Plain Language Address

PM —Program Manager

PME —Professional Military Education

POC —Point of Contact

POW —Prisoner of War

PR —Personnel Recovery; Production Requirement

RST —Reserve Support Team

Q-DUC —Quick Dial-Up Capability

RAM —Reserve Affairs Manager

RASP —Remote Access Secure Program

R/R —Retirement/Retention

RCC —Rescue Coordination Center

RF —Radio Frequency

RFI —Request for Information

RPO —Reserve Pay Office

RT —Resistance Training

RWR —Radar Warning Receiver

SAC —Strategic Air Command

SAFE —Selected Area for Evasion

SAID —Selected Area for Evasion Intelligence Description

SAM —Surface-to-Air Missile

SAR —Search and Rescue; Synthetic Aperture Radar

SARNEG —Search and Rescue Numeric Encryption Grid

SATCOM —Satellite Communications

SAV —Staff Assistance Visit

SCI —Sensitive Compartmented Information

SCIF —Sensitive Compartmented Information Facility

SDD —Secure Data Device

SEA —South East Asia

SERE —Survival, Evasion, Resistance and Escape

SF —Security Forces

SFS —Security Forces Squadron

SIDL —Standard Intelligence Document Listing

SII —Statement of Intelligence Interest

SIMO —Systems Integration Management Office

SIO —Senior Intelligence Officer

SIOP —Single Integrated Operational Plan

SIPRNET —SECRET Internet Protocol Router Network

SIR —Spectrum Interference Resolution

SOUTHCOM —Southern Command

SPINS —Special Instructions

SSAN —Social Security Account Number

SSBI —Single Scope Background Investigation

SSO —Special Security Office or Officer

SSR —Special Security Representative

STU-III —Secure Telephone Unit-III

TACC —Tanker Airlift Control Center

TALCE —Tactical Airlift Control Element

TALO —Tactical Airlift Liaison Officer

TDY —Temporary Duty

TIBS —Tactical Information Boxes; Tactical Information Broadcast Service

TOT —Time over Target

TRANSEC —Transmission Security

TRAP —Tactical Receive Applications

TRE —Tactical Receive Equipment

TTP —Tactics, Techniques, and Procedures

TWG —Threat Working Group

UCMJ —Uniform Code of Military Justice

UDM —Unit Deployment Manager

UHF —Ultra-High Frequency

UIF —Unfavorable Information File

ULAP —Unit-Level Adaptive Planning System

UMB —Unit Mission Brief

UMD —Unit Manning Document

UPMR —Unit Personnel Management Roster

USAFE —United States Air Forces Europe

USCENTAF —United States Central Command Air Forces

USCENTCOM —United States Central Command

USMTF —United States Message Text Format

USSOUTHCOM —United States Southern Command

USSPACECOM —United States Space Command

USSTRATCOM —United States Strategic Command

UTC —Unit Type Code

UTM —Universal Transverse Mercator

VFR —Visual Flight Rules

VHF —Very High Frequency

VRAD —Visual Risk Assessment Database

VTA —Virtual Risk Assessor

VTC —Video-Teleconference

WOC —Wing Operations Center

WOTS —Web Order Transaction System